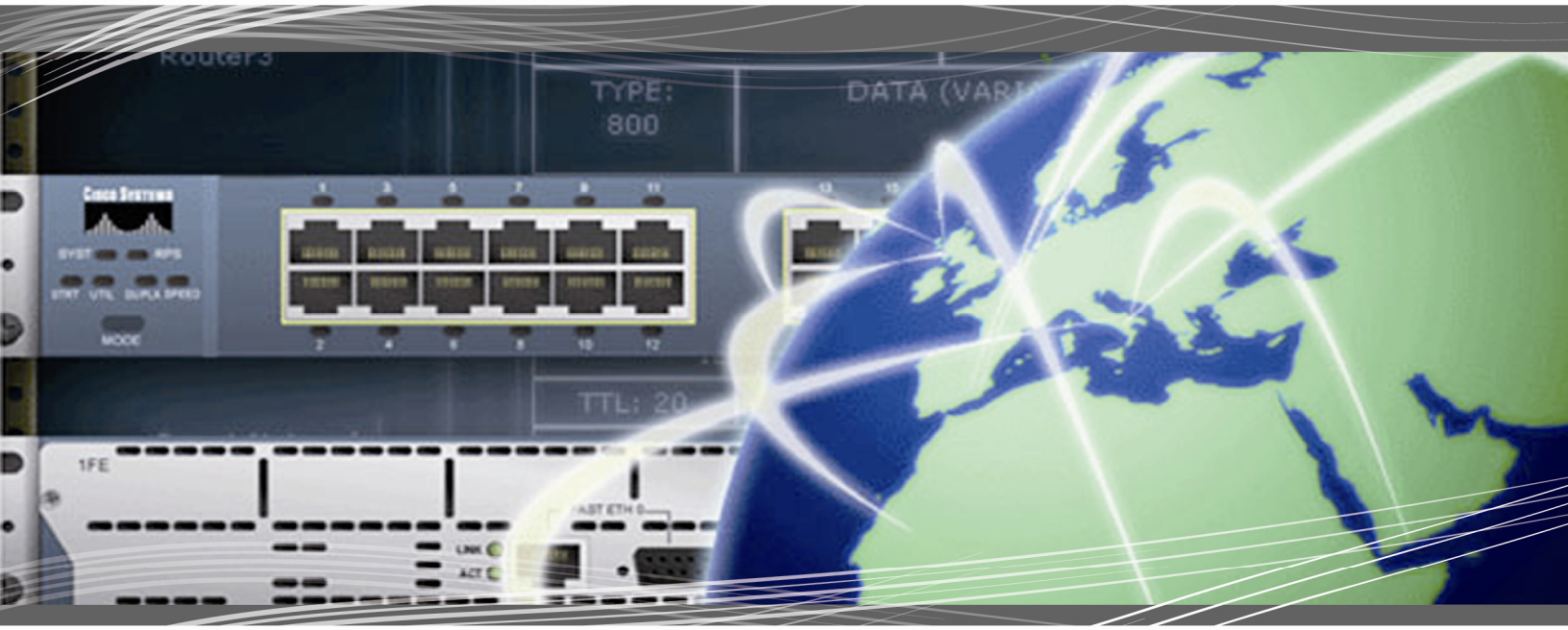
Cisco | Networking Academy®
Mind Wide Open™

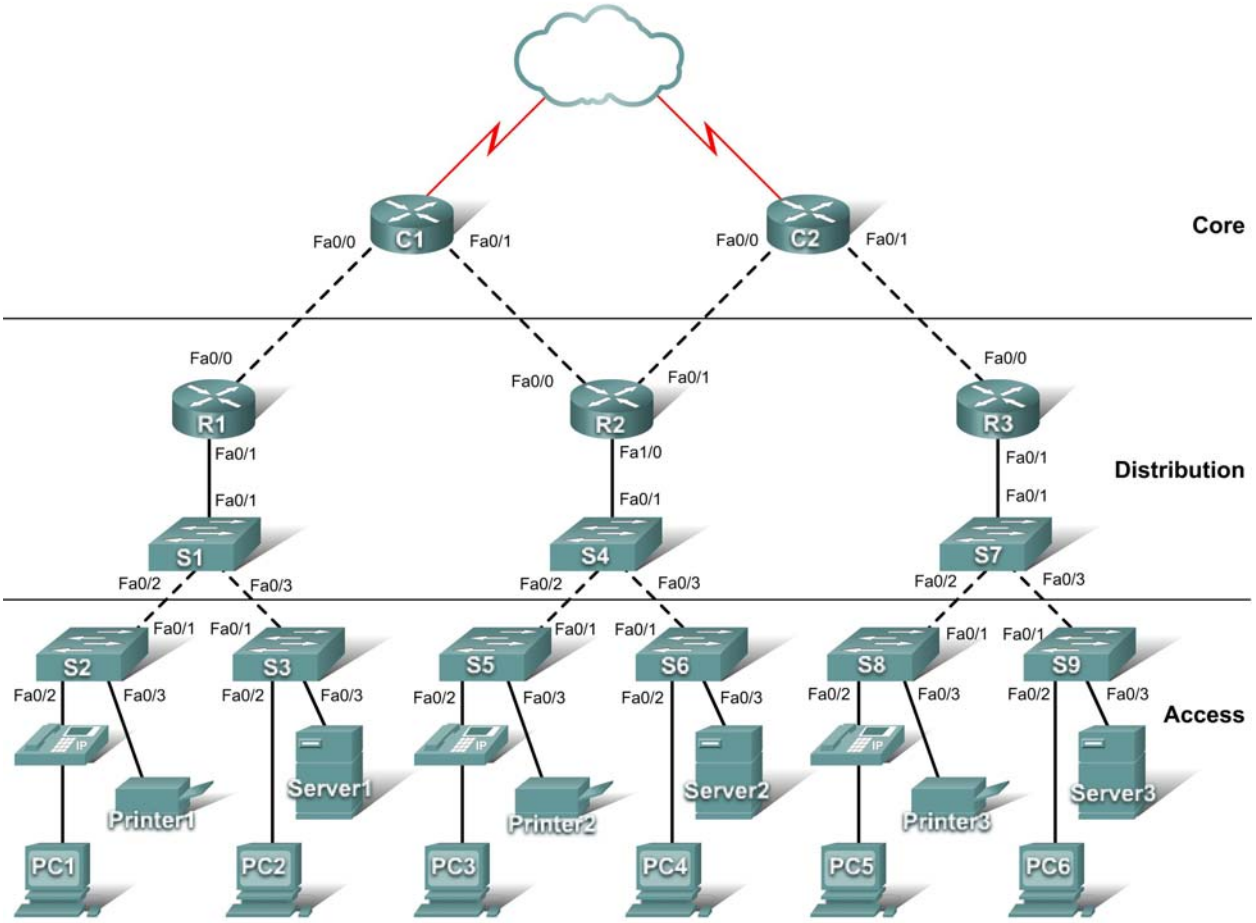


CCNA Exploration 4.0

LAN Switching and Wireless
Student Packet Tracer Manual

PT Activity 1.2.4: Build a Hierarchical Topology

Topology Diagram



Learning Objectives

- Add devices to a topology
- Connect the devices

Introduction

Packet Tracer is integrated throughout this course. You must know how to navigate the Packet Tracer environment to complete this course. Use the tutorials if you need a review of Packet Tracer fundamentals. The tutorials are located in the Packet Tracer **Help** menu.

This activity focuses on building a hierarchical topology, from the core to the distribution and access layers.

Task 1: Add Devices to the Topology

Step 1. Add the missing distribution layer routers and switches.

- The routers you need are located in Custom Made Devices. R1 and R3 are 1841 routers. Ctrl-click the 1841 router to add more than one. Press ESC to cancel. R2 is a 2811 router.
- Now add the S1, S2, and S3 distribution layer switches using the 2960-24TT model

Step 2. Add the remaining access layer switches.

Following the topology diagram, add 2960-24TT switches to complete the rest of the access layer. Remember you can use press Ctrl-click to add multiple devices of the same type.

Step 3. Change the display name for each new device.

- Click a device to open its configuration window.
- Select the **Config** tab to access the basic configuration options.
- In Global Settings under Display Name and Hostname, type the name for the device shown in the topology diagram.
- Repeat the process for all the new devices that you added.

Although Packet Tracer does not grade adding the display names, this step must be completed to successfully complete this activity.

Step 4. Check results.

Your completion percentage should be 14%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Connect the Devices

Pay close attention to the topology diagram and the labeled interfaces when connecting the devices. You are graded on the connections. For instance, in the topology diagram switch S1 is connected to R1 through interface Fa0/1 on both sides. This connection is scored on both the cable type and interface designation. Do not use the Smart Connection utility to make these connections because you have no control over which interface is selected.

Step 1. Cable the core layer routers to the distribution layer routers.

- Using copper crossover cables, connect the core layer routers, C1 and C2, to the distribution layer routers, R1, R2, and R3.
- C1 connects to both R1 and R2, and C2 connects to both R2 and R3.
- As with devices, you can Ctrl-click the cable type to make multiple connections without having to re-select the cable.
- Remember to refer to the topology diagram to determine which interfaces to use for these connections.

Step 2. Cable the distribution layer routers to the access layer switches.

Connect the distribution layer routers to the access layer switches using copper straight-through cables. R1 connects to S1, R2 connects to S4, and R3 connects to S7.

Step 3. Cable the access layer switches.

Connect the access layer switches using copper crossover cables. Follow the topology diagram for the correct connections.

Step 4. Cable the end devices.

Connect the remaining end devices (IP phones, printers, PCs, and servers) to the correct switch using copper straight-through cables. When connecting a switch to a PC, remember to connect to the Fast Ethernet port of the PC.

Step 5. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Note: A bug in Packet Tracer may cause your percentage to show only 99% even though all the required components are complete. If you wait long enough, Packet Tracer eventually catches up and gives you the full 100%.

Step 6. Reflection.

Notice that the link lights for ports between switches and between a switch and an end device eventually transition from amber to green. Why are the link lights for ports between routers and for ports between routers and switches red?

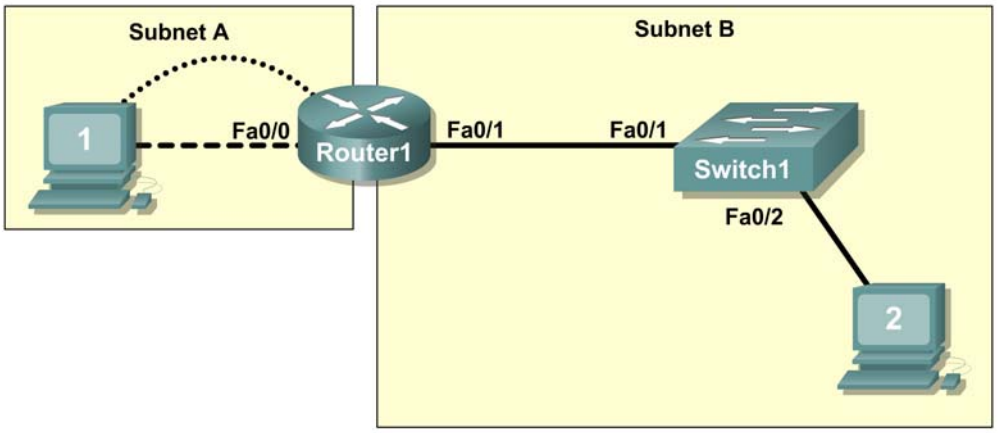
_____

_____

_____

PT Activity 1.3.1: Review of Concepts from Exploration 1

Topology Diagram



Learning Objectives

- Design a logical LAN topology
- Configure the physical topology
- Configure the logical topology
- Verify network connectivity
- Verify passwords

Introduction

In this activity, you will design and configure a small routed network and verify connectivity across multiple network devices. This requires creating and assigning two subnetwork blocks, connecting hosts and network devices, and configuring host computers and one Cisco router for basic network connectivity. Switch1 has a default configuration and does not require additional configuration. You will use common commands to test and document the network. The zero subnet is used.

Task 1: Design a Logical LAN Topology

Step 1. Design an IP addressing scheme.

Given the IP address block of 192.168.7.0 /24, design an IP addressing scheme that satisfies the following requirements:

Subnet	Number of Hosts
Subnet A	**110**
Subnet B	**54**

The 0 subnet is used. No subnet calculators may be used. Create the smallest possible subnets that satisfy the requirements for hosts. Assign the first usable subnet to Subnet A.

Host computers will use the first IP address in the subnet. The network router will use the last IP address in the subnet.

Step 2. Write down the IP address information for each device.

Before proceeding, verify your IP addresses with the instructor.

Task 2: Configure the Physical Topology

Step 1. Cable the network.

- Connect Host1 to the Fa0/0 interface on Router1
- Connect a console cable between Host1 and Router1
- Connect the Fa0/1 interface on Switch1 to the Fa0/1 interface on Router1
- Connect Host2 to the Fa0/2 interface on Switch1

Step 2. Inspect the network connections.

Verify the connections visually.

Task 3: Configure the Logical Topology

Step 1. Configure the host computers.

Configure the static IP address, subnet mask, and gateway for each host computer.

Step 2. Configure Router1.

Connect to Router1 through the Terminal connection on Host1. Enter the following commands on the router:

Remember: Packet Tracer is case sensitive when it grades the **description** command.

```
Router>enable
Router#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#enable secret class
Router1(config)#line console 0
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#line vty 0 4
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#int fa0/0
Router1(config-if)#ip address addr sub_mask !Supply your answer from Task 1
Router1(config-if)#no shutdown
Router1(config-if)#description connection to host1
Router1(config-if)#interface fa0/1
Router1(config-if)#description connection to switch1
Router1(config-if)#ip address addr sub_mask !Supply your answer from Task 1
Router1(config-if)#no shutdown
Router1(config-if)#end
Router1#
```


Task 4: Verify Network Connectivity

Step 1. Use the ping command to verify network connectivity.

You can verify network connectivity using the **ping** command.

Task 5: Verify Passwords

Step 1. Telnet to the router from Host2 and verify the Telnet password.

You should be able to telnet to either Fast Ethernet interface of the router.

In a command window on Host 2, type:

```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.7.190
Trying 192.168.7.190 ...

User Access Verification

Password:
```

When you are prompted for the Telnet password, type **cisco** and press Enter.

Step 2. Verify that the enable secret password has been set.

From the Telnet session, enter privilege exec mode and verify it is password protected:

```
Router1>enable
```

Were you prompted for the enable secret password?

Task 6: Reflection

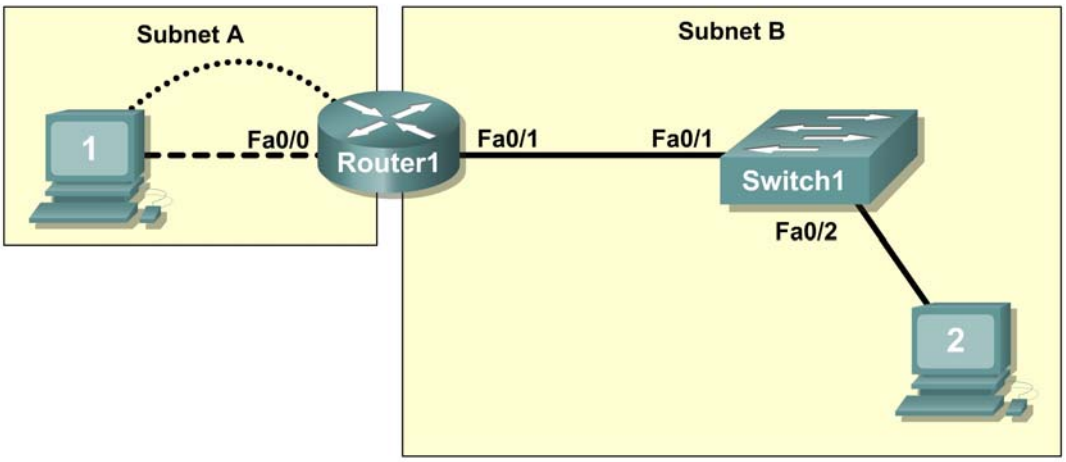
How are Telnet access and console access different?

When might it make sense to set different passwords on these two access ports?

Why does the switch between Host2 and the router not require configuration with an IP address to forward packets?

PT Activity 1.3.2: Review of Concepts from Exploration 1 - Challenge

Topology Diagram



Learning Objectives

- Design a logical LAN topology
- Configure the physical topology
- Configure the logical topology
- Verify network connectivity
- Verify passwords

Introduction

In this activity, you will design and configure a small routed network and verify connectivity across multiple network devices. This requires creating and assigning two subnetwork blocks, connecting hosts and network devices, and configuring host computers and one Cisco router for basic network connectivity. Switch1 has a default configuration and does not require additional configuration. You will use common commands to test and document the network. The zero subnet is used.

Task 1: Design a Logical LAN Topology

Step 1. Design an IP addressing scheme.

Given the IP address block of **192.168.30.0 /27**, design an IP addressing scheme that satisfies the following requirements:

Subnet	Number of Hosts
Subnet A	**7**
Subnet B	**14**

The 0 subnet is used. No subnet calculators may be used. Create the smallest possible subnets that satisfy the requirements for hosts. Assign the first usable subnet to Subnet A.

Host computers will use the first IP address in the subnet. The network router will use the last IP address in the subnet.

Step 2. Write down the IP address information for each device.

Before proceeding, verify your IP addresses with the instructor.

Task 2: Configure the Physical Topology

Step 1. Cable the network.

Step 2. Inspect the network connections.

Task 3: Configure the Logical Topology

Step 1. Configure the host computers.

Step 2. Configure Router1.

Enter the following commands on the router:

- Router name **Router1**
- Secret password **class**
- Set console and VTY line passwords to **cisco**
- Interface addresses
- Interface description
    - Fa0/0 text: connection to host1
    - Fa0/1 text: connection to swtich1

Task 4: Verify Network Connectivity

Step 1. Use the ping command to verify network connectivity.

You can verify network connectivity using the **ping** command.

Task 5: Verify Passwords

Step 1. Telnet to the router from Host2 and verify the Telnet password.

Step 2. Verify that the enable secret password has been set.

Task 6: Reflection

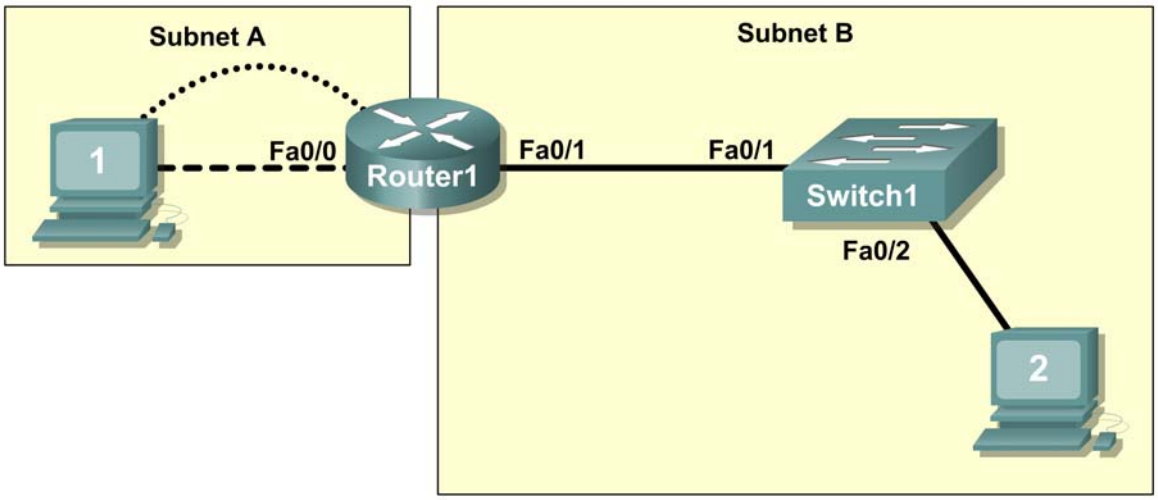
How are Telnet access and console access different?

When might it make sense to set different passwords on these two access ports?

Why does the switch between Host2 and the router not require configuration with an IP address to forward packets?

PT Activity 1.3.3: Troubleshooting a Small Network

Topology Diagram



Learning Objectives

- Examine the logical LAN topology
- Troubleshoot network connections

Introduction

The configuration contains design and configuration errors that conflict with stated requirements and prevent end-to-end communication. You will troubleshoot the connectivity problems to determine where the errors are occurring and correct them using the appropriate commands. When all errors have been corrected, each host should be able to communicate with all other configured network elements and with the other host.

Task 1: Examine the Logical LAN Topology

Step 1. Design an IP addressing scheme.

The IP address block of **172.16.30.0 /23** is subnetted to meet the following requirements:

Subnet	Number of Hosts
Subnet A	**174**
Subnet B	**60**

Additional requirements and specifications:

- The 0 subnet is used.
- The smallest possible number of subnets that satisfy the requirements for hosts should be used, keeping the largest possible block in reserve for future use.
- Assign the first usable subnet to Subnet A.
- Host computers use the first IP address in the subnet.
- The network router uses the last network host address.

Based on these requirements, the following addressing requirements have been provided to you:

Subnet A	
IP mask (decimal)	**255.255.255.0**
IP address	**172.16.30.0**
First IP host address	**172.16.30.1**
Last IP host address	**172.16.30.254**
Subnet B	
IP mask (decimal)	**255.255.255.128**
IP address	**172.16.31.0**
First IP host address	**172.16.31.1**
Last IP host address	**172.16.31.126**

Examine each of the values in the tables above and verify that this topology meets all requirements and specifications. Are any of the given values incorrect?

If yes, make note of the corrected values.

Task 2: Troubleshoot Network Connections

Step 1. Begin troubleshooting at the host connected to the BRANCH router.

From host PC1, is it possible to ping PC2?

From host PC1, is it possible to ping the router fa0/1 interface?

From host PC1, is it possible to ping the default gateway?

From host PC1, is it possible to ping itself?

Where is the most logical place to begin troubleshooting the PC1 connection problems?

Step 2. Examine the router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

If there are problems with the status of the interfaces, record any commands that are necessary to correct the configuration errors.

Step 3. Use the necessary commands to correct the router configuration.

Step 4. View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces.

Does the information in the interface status summary indicate any configuration errors on Router1?

If the answer is yes, troubleshoot the interface status of the interfaces.

Has connectivity been restored?

Step 5. Verify the logical configuration.

Examine the full status of Fa 0/0 and 0/1. Is the IP addresses and subnet mask information in the interface status consistent with the configuration table?

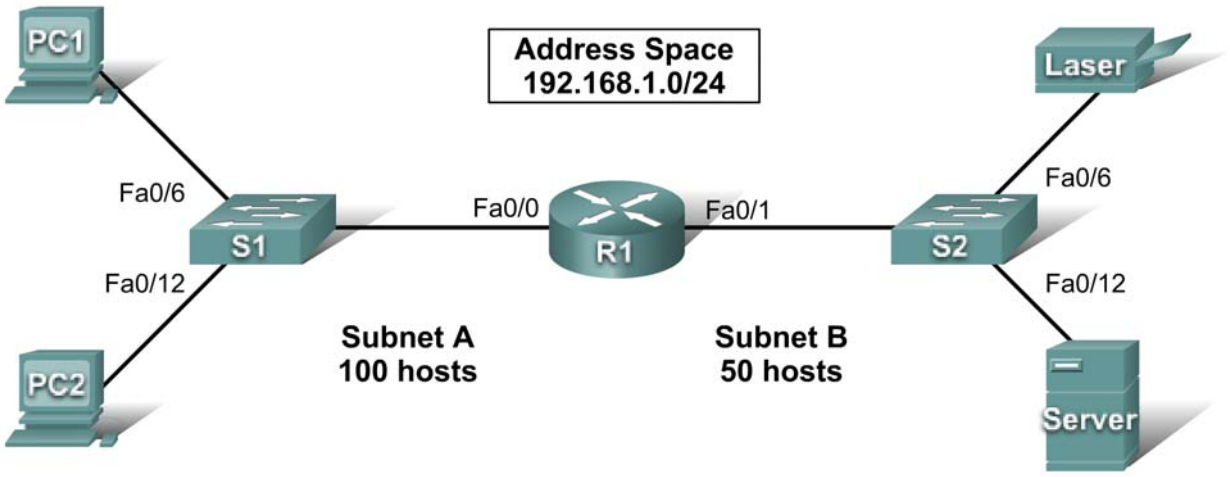
If there are differences between the configuration table and the router interface configuration, record any commands that are necessary to correct the router configuration.

Has connectivity been restored?

Why is it useful for a host to ping its own address?

PT Activity 1.4.1: Packet Tracer Skills Integration Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**			N/A
	Fa0/1			N/A
PC1	**NIC**			
PC2	**NIC**			
Laser	**NIC**			
Server	**NIC**			

Learning Objectives

- Design the network
- Build the network
- Apply a basic configuration
- Test connectivity

Introduction

This activity reviews the skills you acquired in the Exploration: Network Fundamentals course. The skills include subnetting, building a network, applying an addressing scheme, and testing connectivity. You should review those skills before proceeding. In addition, this activity reviews the basics of using the Packet Tracer program. Packet Tracer is integrated throughout this course. You must know how to

navigate the Packet Tracer environment to complete this course. Use the tutorials if you need a review of Packet Tracer fundamentals. The tutorials are located in the Packet Tracer **Help** menu.

Task 1: Design and Document an Addressing Scheme

Step 1. Design an addressing scheme.

Using the 192.168.1.0/24 address space, design an addressing scheme according to the following requirements:

Subnet A

- Subnet the address space to provide for 100 hosts
- Assign the Fa0/0 interface the first useable IP address.
- Assign PC1 the second useable IP address.
- Assign PC2 the last useable IP address in the subnet.

Subnet B

- Subnet the remaining address space to provide for 50 hosts
- Assign the Fa0/1 interface the first useable IP address.
- Assign the laser printer the second useable IP address.
- Assign the server the last useable IP address in the subnet.

Step 2. Document the addressing scheme.

Complete an addressing table for the router and each end device in the network.

Task 2: Add and Connect the Devices

Step 1. Add the necessary equipment.

Add the following devices to the network. For placement of these devices, refer to the topology diagram.

- Two 2960-24TT switches
- One 1841 router
- Two generic PCs
- One generic server
- One generic printer

Step 2. Name the devices.

Change the Display Name and Hostname to match the device names shown in the topology diagram. Device names are case-sensitive.

Step 3. Connect the devices.

Use the following specifications for the connections between the devices:

- S1 Fa0/1 to R1 Fa0/0
- S1 Fa0/6 to PC1
- S1 Fa0/12 to PC2
- S2 Fa0/1 to R1 Fa0/1

- S2 Fa0/6 to Laser
- S2 Fa0/12 to Server

Step 4. Check results.

Your completion percentage should be 46%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Apply Basic Configurations

Step 1. Configure the router.

- The privileged EXEC secret password is **class**.
- The banner is **Authorized Access Only**.
- The line password is **cisco** for console and telnet.
- Configure the appropriate interfaces. Use the following descriptions:
  - **Link to PC LAN**
  - **Link to Server & Printer**

Note: Remember that the banner and descriptions are case-sensitive. Do not forget to activate the interfaces.

Step 2. Configure the end devices.

Step 3. Check results.

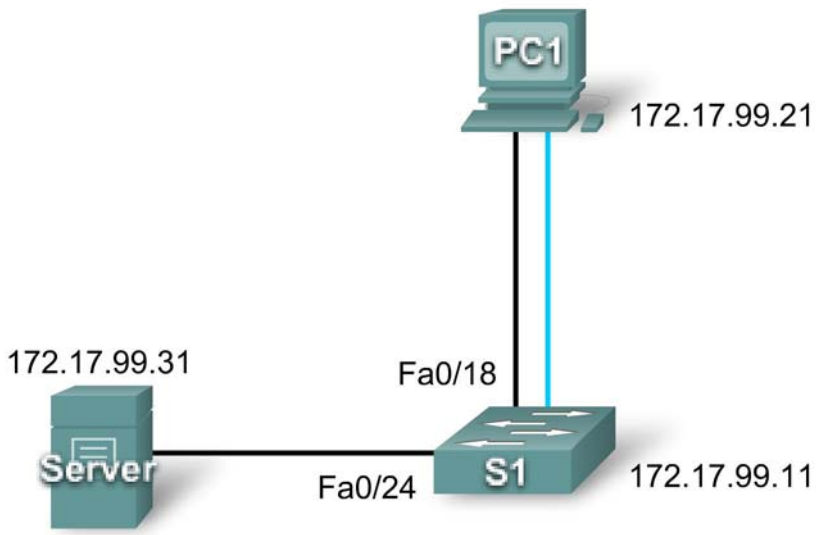
Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Test Connectivity and Examine the Configuration

You should now have end-to-end connectivity, which means every end device should be reachable from any other end device. From PC1 and PC2, ping all end devices on the network. If you get an error, try pinging again to make sure ARP tables are updated. If you still receive an error, check your subnetting, the cables, and the IP addresses. Isolate problems and implement solutions.

PT Activity 2.3.8: Configuring Basic Switch Management

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	**VLAN99**	172.17.99.11	255.255.255.0
PC1	**NIC**	172.17.99.21	255.255.255.0
Server	**NIC**	172.17.99.31	255.255.255.0

Learning Objectives

- Connect to the switch using a console connection
- Navigate through various CLI modes
- Use the Help Facility to configure the clock
- Access and configure command history
- Configure the boot sequence
- Configure a PC and connect it to a switch
- Configure full duplex
- Manage the MAC address table
- Manage the switch configuration file

Introduction

Basic switch management is the foundation for configuring switches. This activity focuses on navigating command-line interface modes, using help functions, accessing the command history, configuring boot

sequence parameters, setting speed and duplex settings, as well as managing the MAC address table and switch configuration file. Skills learned in this activity are necessary for configuring basic switch security in later chapters.

Task 1: Connect to the Switch

Step 1: Connect S1 and PC1.

- Using a console cable, connect the RS 232 interface on PC1 to the console interface on switch S1.
- Click **PC1** and then click the **Desktop** tab. Select **Terminal** in the Desktop tab.
- Keep these default settings for Terminal Configuration and then click **OK**:

  Bits Per Second = 9600
  Data Bits = 8
  Parity = None
  Stop Bits = 1
  Flow Control = None
- You are now consoled into S1. Press **Enter** to get the Switch prompt.

Step 2: Check results.

Your completion percentage should be 6%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Navigate Through CLI Modes

Step 1: In user EXEC mode, type ?. Note the list of available commands.

While in user EXEC mode, the available commands are limited to basic monitoring commands.

Step 2: Use the enable command to go to privileged EXEC mode.

```
Switch>enable
Switch#
```

The prompt changes from **>** to **#**.

Step 3: In privileged EXEC mode, type ?. Note the list of available commands.

There are now more available commands compared to user EXEC mode. In addition to the basic monitoring commands, configuration and management commands can now be accessed.

Step 4: Change to global configuration mode.

```
Switch#configure terminal
Switch(config)#
```

Step 5: In global configuration mode, type ?. Note the list of available commands.

Step 6: Configure S1 as the hostname.

```
Switch(config)#hostname S1
S1(config)#
```


Step 7: Change to interface configuration mode for VLAN99.

The **interface vlan 99** command creates the interface and changes to interface configuration mode for VLAN99.

```
S1(config)#interface vlan 99
S1(config-if)#
```

Step 8: Configure VLAN99 with 172.17.99.11/24 and activate the interface.

Use the **ip address** and **no shutdown** commands to assign the correct IP address/subnet mask and activate the interface.

```
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
```

Step 9: Change to interface configuration mode for Fa0/18.

```
S1(config-if)#interface fa0/18
S1(config-if)#
```

Step 10: Set the port mode to access.

To allow for frames to be sent and received from the interface, change the switching mode to access using the **switchport mode access** command.

```
S1(config-if)#switchport mode access
```

Step 11: Assign VLAN99 to the port.

To allow the Fa0/18 interface to act as a member of VLAN 99, issue the **switchport access vlan 99** command.

```
S1(config-if)#switchport access vlan 99
```

Step 12: Exit interface configuration mode.

Issue the **exit** command to leave interface configuration mode and enter global configuration mode.

Step 13: Enter configuration mode for the console line.

```
S1(config)#line console 0
S1(config-line)#
```

Step 14: In line configuration mode, type ?. Note the list of available commands.

Step 15: Enter cisco as the password and require users to login.

```
S1(config-line)#password cisco
S1(config-line)#login
```

Step 16: Return to privileged EXEC mode using the end command.

```
S1(config-line)#end
S1#
```

Step 17: Check results.

Your completion percentage should be 31%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Use Help Facility to Configure the Clock

Step 1: At the privileged EXEC command prompt, type clock ?.

```
S1#clock ?
```

The only option is **set**.

Step 2: Use Help to assist setting the clock to the current time.

```
S1#clock ?
  set  Set the time and date

S1#clock set ?
  hh:mm:ss Current Time

S1#clock set 12:12:12 ?
  <1-31>  Day of the month
  MONTH   Month of the year
```

Continue issuing the **?** command until you have completed configuring the clock. You are warned with a **% Incomplete command message** if the **clock** command is not fully entered with all the required arguments.

Step 3: Verify that the clock is set.

To verify that the clock is set, issue the **show clock** command.

Note: Packet Tracer does not always show the correct time configured.

Completion is still at 31% at the end of this Task.

Task 4: Access and Configure Command History

Step 1: View the most recent commands entered.

Issue the **show history** command. Remember how many commands are listed.

```
S1#show history
```

Step 2: Change the number of commands stored in the history buffer.

Enter line configuration mode for both the console and Telnet lines. Set the number of commands held in the history buffer to 35.

```
S1(config)#line console 0
S1(config-line)#history size 35
S1(config-line)#line vty 0 4
S1(config-line)#history size 35
```

Step 3: Verify that the size of the history buffer has changed.

Return to privileged EXEC mode and issue the **show history** command again. There should be more commands displayed than previously.

Step 4: Check results.

Your completion percentage should be 50%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure the Boot Sequence

Step 1: Check which Cisco IOS software version is currently loaded.

```
S1#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
<output omitted>
```

The version is listed in the first line.

Step 2: Check which Cisco IOS images are loaded in flash memory.

```
S1#show flash
Directory of flash:/

    3  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    2  -rw-     4670455          <no date>  c2960-lanbase-mz.122-25.SEE1.bin
    6  -rw-         616          <no date>  vlan.dat

32514048 bytes total (23428056 bytes free)
S1#
```

Note that there are two versions in flash memory. The version that is currently loaded is **c2960-lanbase-mz.122-25.FX.bin**.

Step 3: Configure the system to boot using a different Cisco IOS image.

In global configuration mode, issue this command.

```
S1(config)#boot system flash:/c2960-lanbase-mz.122-25.SEE1.bin
```

Note: Although you can enter this command in Packet Tracer, the switch still loads the first image listed in flash.

Packet Tracer does not grade the **boot system** command on switches, so completion remains at 50% at the end of this task.

Task 6: Configure a PC and Connect it to a Switch

Step 1: Configure PC1 with the IP address/subnet mask 172.17.99.21/24.

- Exit the terminal to return to the **Desktop** tab.
- Click **IP Configuration** and set the IP address to 172.17.99.21 and subnet mask to 255.255.255.0

Step 2: Connect PC1 to Fa0/18 on the switch.

Using the copper straight-through cable, connect the FastEthernet port of the PC to the Fa0/18 port on the switch.

Step 3: Test connectivity between S1 and PC1.

Ping between S1 and PC1. It may take a few attempts, but it should be successful.

Step 4: Check results.

Your completion percentage should be 69%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure Duplex and Speed

Step 1: Use the Config tab change the settings.

On PC1, select the **Config** tab. Set the bandwidth of the FastEthernet interface to 100 Mbps and Full Duplex.

Step 2: Use Cisco IOS commands to set Fa0/18.

Return to the desktop and select **Terminal**, and then configure the interface.

```
S1(config)#interface fa0/18
S1(config-if)#duplex full
S1(config-if)#speed 100
```

Step 3: Test connectivity between S1 and PC1.

Issue a ping from S1 to PC1. It may take a few attempts, but it should be successful.

Step 4: Check results.

Your completion percentage should be 81%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Manage the MAC Address Table

Step 1: Check the MAC address of the server.

Click the **Server**, then the **Config** tab, and then **FastEthernet**. The MAC Address is 0060.3EDD.19A3.

Step 2: Configure static MAC for the TFTP server.

By configuring a static MAC for the TFTP server, the switch always knows which port to use to send out traffic destined for the server. In global configuration mode on S1, add the MAC address to the addressing table of the switch:

```
S1(config)#mac-address-table static 0060.3EDD.19A3 vlan 99 int fa0/24
```

Step 3: Verify that the static MAC address is now in the MAC address table.

```
S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0060.3edd.19a3    STATIC      Fa0/24
  99    0060.5c5b.cd23    DYNAMIC     Fa0/18
S1#
```

Notice how the MAC address from PC1 was added dynamically. This entry may or may not be in your table depending on how long it has been since you pinged from PC1 to S1.

Step 4: Test connectivity between S1 and PC1.

Issue a ping from S1 to PC1. It may take a few attempts, but the command should be successful.

Packet Tracer does not grade this command. This command is needed to allow the switch to know where to send traffic destined for the server. Completion is still at 81% at the end of this task.

Task 9: Manage the Switch Configuration File

Using a copper straight-through cable, connect the FastEthernet port on the server to the Fa0/24 port on the switch.

Step 1: Enter interface configuration mode for Fa0/24.

```
S1#configure terminal
S1(config)#interface fa0/24
S1(config-if)#
```

Step 2: Set the port mode to access.

Setting the port mode to access allows frames to be sent and received from the interface.

```
S1(config-if)#switchport mode access
```

Note: Packet Tracer does not grade the **switchport mode access** command. However, the command is needed to change the interface from its default mode to access mode.

Step 3: Assign VLAN99 to the port.

Assigning VLAN99 to the port allows the Fa0/24 interface to act as a member of VLAN 99.

```
S1(config-if)#switchport access vlan 99
```

Step 4: Verify S1 can ping the server.

Ping the server from S1. It may take a few attempts, but it should be successful.

Step 5: Back up the startup configuration to the server.

In privileged EXEC mode, copy the startup configuration to the sever. When you are prompted for the address of the remote host, enter IP address of the server, 172.17.99.31. For the destination filename, use the default filename by pressing **Enter**.

```
S1#copy startup-config tftp:
Address or name of remote host []? 172.17.99.31
Destination filename [S1-confg]? [Enter]
```

Step 6: Verify that the server has the startup configuration.

To determine if the startup configuration was successfully transferred to the server, click the server and then click the **Config** tab. The S1-confg file should be listed under Services and TFTP.

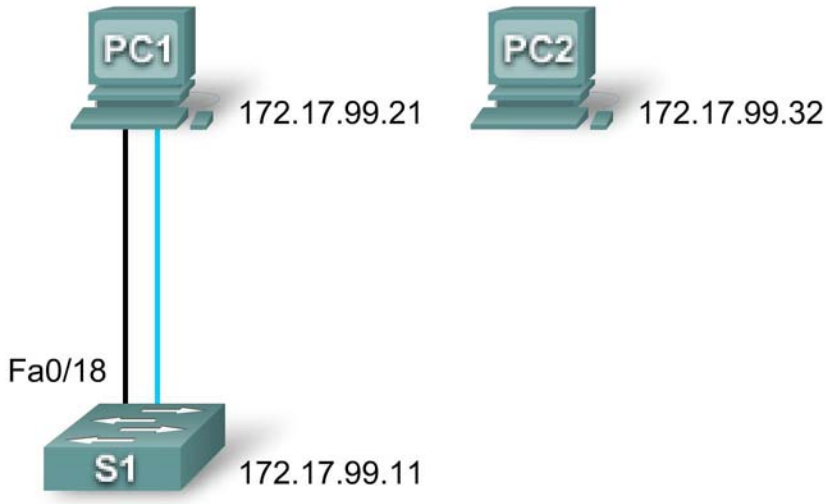
Note: Restoring the startup from the server is not fully simulated in Packet Tracer.

Step 7: Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 2.4.7: Configure Switch Security

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	**VLAN99**	172.17.99.11	255.255.255.0
PC1	**NIC**	172.17.99.21	255.255.255.0
PC2	**NIC**	172.17.99.32	255.255.255.0

Learning Objectives

- Configure basic switch management
- Configure dynamic port security
- Test dynamic port security
- Secure unused ports

Task 1: Configure Basic Switch Management

Step 1: From PC1, access the console connection to S1.

- Click PC1 and then the Desktop tab. Select Terminal in the Desktop tab.
- Keep these default settings for Terminal Configuration and then click OK:

  Bits Per Second = 9600
  Data Bits = 8
  Parity = None

Stop Bits = 1
Flow Control = None

- You are now consoled into S1. Press Enter to get the Switch prompt.

Step 2: Change to privileged EXEC mode.

To access privileged EXEC mode, type the **enable** command. The prompt changes from **>** to **#**.

```
S1>enable
S1#
```

Notice how you were able to enter privileged EXEC mode without providing a password. Why is the lack of a privileged EXEC mode password a security threat?

_____

_____

_____

Step 3: Change to global configuration mode and configure the privileged EXEC password.

- While in privileged EXEC mode, you can access global configuration mode by using the **configure terminal** command.
- Use the **enable secret** command to set the password. For this activity, set the password to **class**.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret class
S1(config)#
```

Note: PT will not grade the **enable secret** command.

Step 4: Configure virtual terminal and console passwords and require users to login.

A password should be required to access the console line. Even the basic user EXEC mode can provide significant information to a malicious user. In addition, the vty lines must have a password before users can access the switch remotely.

- Access the console prompt using the **line console 0** command.
- Use the **password** command to configure the console and vty lines with **cisco** as the password. Note: PT will not grade the **password cisco** command in this case.
- Then enter the **login** command, which requires users to enter a password before gaining access to user EXEC mode.
- Repeat the process with the vty lines. Use the **line vty 0 15** command to access the correct prompt.
- Type the **exit** command to return to the global configuration prompt.

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```


Step 5: Configure password encryption.

The privileged EXEC password is already encrypted. To encrypt the line passwords that you just configured, enter the **service password-encryption** command in global configuration mode**.**

```
S1(config)#service password-encryption
S1(config)#
```

Step 6: Configure and test the MOTD banner.

Configure the message-of-the-day (MOTD) using **Authorized Access Only** as the text. The banner text is case sensitive. Make sure you do not add any spaces before or after the banner text. Use a delimiting character before and after the banner text to indicate where the text begins and ends. The delimiting character used in the example below is **&,** but you can use any character that is not used in the banner text. After you have configured the MOTD, log out of the switch to verify that the banner displays when you log back in.

```
S1(config)#banner motd &Authorized Access Only&
S1(config)#end [or exit]
S1#exit

S1 con0 is now available

Press RETURN to get started.

[Enter]

Authorized Access Only

User Access Verification

Password:
```

- The password prompt now requires a password to enter user EXEC mode. Enter the password **cisco**.
- Enter privileged EXEC mode with the password **class** and return to global configuration mode with the **configure terminal** command.

```
Password: [cisco] !Note: Password does not display as you type.

S1>enable
Password: [class] !Note: Password does not display as you type.
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
```

Step 7: Check results.

Your completion percentage should be 40%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Dynamic Port Security

Step 1: Enable VLAN99.

Packet Tracer opens with the VLAN 99 interface in the down state, which is not how an actual switch operates. You must enable VLAN 99 with the **no shutdown** command before the interface becomes active in Packet Tracer.


```
S1(config)#interface vlan 99
S1(config-if)#no shutdown
```

Step 2: Enter interface configuration mode for FastEthernet 0/18 and enable port security.

Before any other port security commands can be configured on the interface, port security must be enabled.

```
S1(config-if)#interface fa0/18
S1(config-if)#switchport port-security
```

Notice that you do not have to exit back to global configuration mode before entering interface configuration mode for fa0/18.

Step 3: Configure the maximum number of MAC addresses.

To configure the port to learn only one MAC address, set the **maximum** to **1**:

```
S1(config-if)#switchport port-security maximum 1
```

Note: PT does not grade the **switchport port-security maximum 1** command, however this command is vital in configuring port security.

Step 4: Configure the port to add the MAC address to the running configuration.

The MAC address learned on the port can be added to ("stuck" to) the running configuration for that port.

```
S1(config-if)#switchport port-security mac-address sticky
```

Note: PT does not grade the **switchport port-security mac-address sticky** command, however this command is vital in configuring port security.

Step 5: Configure the port to automatically shut down if port security is violated.

If you do not configure the following command, S1 only logs the violation in the port security statistics but does not shut down the port.

```
S1(config-if)#switchport port-security violation shutdown
```

Note: PT does not grade the **switchport port-security violation shutdown** command, however this command is vital in configuring port security.

Step 6: Confirm that S1 has learned the MAC address for PC1.

Ping from PC1 to S1.

Confirm that S1 now has static MAC address entry for PC1 in the MAC table:

```
S1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0060.5c5b.cd23    STATIC      Fa0/18
```

The MAC address is now "stuck" to the running configuration.

```
S1#show running-config
<output omitted>
interface FastEthernet0/18
 switchport access vlan 99
```



```
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.5C5B.CD23
<output omitted>
S1#
```

Step 7: Check results.

Your completion percentage should be 70%. If not, click **Check Result**s to see which required components are not yet completed.

Task 3: Test Dynamic Port Security

Step 1: Remove the connection between PC1 and S1 and connect PC2 to S1.

- To test port security, delete the Ethernet connection between PC1 and S1. If you accidentally delete the console cable connection, simply reconnect it.
- Connect PC2 to Fa0/18 on S1. Wait for the amber link light to turn green and then ping from PC2 to S1. The port should then automatically shut down.

Step 2: Verify that port security is the reason the port is shut down.

To verify that port security has shut the port down, enter the command **show interface fa0/18**.

```
S1#show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0090.213e.5712 (bia 0090.213e.5712)
<output omitted>
```

The line protocol is down because of an error (**err**) of accepting a frame with a different MAC address than the learned MAC address, so the Cisco IOS software shut down (**disabled**) the port.

You can also verify a security violation with the **show port-security interface fa0/18** command.

```
S1#show port-security interface fa0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.F7B0.086E:99
Security Violation Count   : 1
```

Notice that the Port Status is **secure-shutdown,** and the security violation count is **1**.

Step 3: Restore the connection between PC1 and S1 and reset port security.

Remove the connection between PC2 and S1. Reconnect PC1 to the Fa0/18 port on S1.

Notice that the port is still down even though you reconnected the PC that is allowed on the port. A port that is in the down state because of a security violation must be manually reactivated. Shut down the port and then activate it with **no shutdown**.

```
S1#config t
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fa0/18
S1(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config-if)#exit
S1(config)#
```

Step 4: Test connectivity by pinging S1 from PC1.

The ping from PC1 to S1 should be successful.

Your completion percentage should still be 70% at the end of this task.

Task 4: Secure Unused Ports

A simple method many administrators use to help secure their network from unauthorized access is to disable all unused ports on a network switch.

Step 1: Disable interface Fa0/17 on S1.

Enter interface configuration mode for FastEthernet 0/17 and shut down the port.

```
S1(config)#interface fa0/17
S1(config-if)#shutdown
```

Step 2: Test the port by connecting PC2 to Fa0/17 on S1.

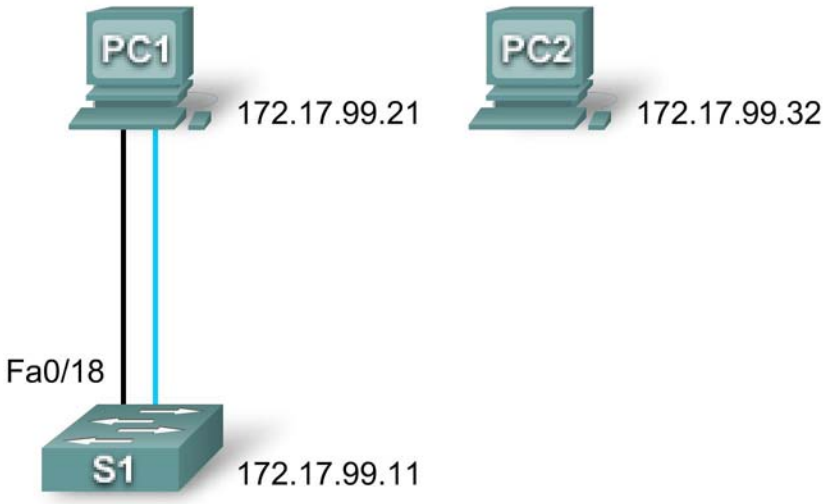
Connect PC2 to the Fa0/17 interface on S1. Notice that the link lights are red. PC2 does not have access to the network.

Step 3: Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 2.5.1: Basic Switch Configuration

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	**NIC**	172.17.99.21	255.255.255.0	172.17.99.11
PC2	**NIC**	172.17.99.22	255.255.255.0	172.17.99.11
S1	**VLAN99**	172.17.99.11	255.255.255.0	172.17.99.1

Learning Objectives

- Clear an existing configuration on a switch
- Verify the default switch configuration
- Create a basic switch configuration
- Manage the MAC address table
- Configure port security

Introduction

In this activity, you will examine and configure a standalone LAN switch. Although a switch performs basic functions in its default out-of-the-box condition, there are a number of parameters that a network administrator should modify to ensure a secure and optimized LAN. This activity introduces you to the basics of switch configuration.

Task 1: Clear an Existing Configuration on a Switch

Step 1. Enter privileged EXEC mode by typing the enable command.

Click S1 and then the CLI tab. Issue the **enable** command to enter the privileged EXEC mode.

```
Switch>enable
Switch#
```

Step 2. Remove the VLAN database information file.

VLAN database information is stored separately from the configuration files in vlan.dat in flash. To remove the VLAN file, issue the command **delete flash:vlan.dat**

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

Step 3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] [Enter]
[OK]
Erase of nvram: complete
```

Step 4. Verify the VLAN information was deleted.

Verify that the VLAN configuration was deleted using the **show vlan** command.

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   VLAN10                            active
30   VLAN30                            active
1002 fddi-default                      active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

The VLAN information is still on the switch. Follow the next step to clear it.

Step 5. Reload the switch.

At the privileged EXEC mode prompt, enter the **reload** command to begin the process.

```
Switch#reload
Proceed with reload? [confirm] [Enter]

%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

<output omitted>
```



```
Press RETURN to get started! [Enter]

Switch>
```

Task 2: Verify the Default Switch Configuration

Step 1. Enter privileged mode.

You can access all the switch commands in privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained.

```
Switch>enable
Switch#
```

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2. Examine the current switch configuration.

Examine the current running configuration by issuing the **show running-config** command.

How many Fast Ethernet interfaces does the switch have? _____

How many Gigabit Ethernet interfaces does the switch have? _____

What is the range of values shown for the vty lines? _____

Examine the current contents of NVRAM by issuing the **show startup-config** command.

Why does the switch give this response?

_____

Examine the characteristics of the virtual interface VLAN1 by issuing the command **show interface vlan1**.

Is there an IP address set on the switch? _____

What is the MAC address of this virtual switch interface? _____

Is this interface up? _____

Now view the IP properties of the interface using the show ip interface vlan1.

What output do you see? _____

Step 3. Display Cisco IOS information.

Display Cisco IOS information using the **show version** command.

What is the Cisco IOS version that the switch is running? _____

What is the system image filename? _____

What is the base MAC address of this switch? _____

Step 4. Examine the Fast Ethernet interfaces.

Examine the default properties of the Fast Ethernet interface used by PC1 using the **show interface fastethernet 0/18** command.

```
Switch#show interface fastethernet 0/18
```

Is the interface up or down? _____

What event would make an interface go up? _____

What is the MAC address of the interface? _____

What is the speed and duplex setting of the interface? _____

Step 5. Examine VLAN information.

Examine the default VLAN settings of the switch using the **show vlan** command.

What is the name of VLAN 1? _____

Which ports are in this VLAN? _____

Is VLAN 1 active? _____

What type of VLAN is the default VLAN? _____

Step 6. Examine flash memory.

There are two commands to examine flash memory, **dir flash:** or **show flash**. Issue either one of the commands to examine the contents of the flash directory.

Which files or directories are found?

_____

Step 7. Examine and save the startup configuration file.

Earlier in step 2 you saw that the startup configuration file did not exist. Make one configuration change to the switch and then save it. Type the following commands:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
```

To save the contents of the running configuration file to non-volatile RAM (NVRAM), issue the the command **copy running-config startup-config**.

```
Switch#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Now display the contents of NVRAM. The current configuration has been written to NVRAM.

Task 3: Create a Basic Switch Configuration

Step 1. Assign a name to the switch.

Enter global configuration mode. Configuration mode allows you to manage the switch. Enter the configuration commands, one on each line. Notice that the command line prompt changes to reflect the current prompt and switch name. In the last step of the previous task, you configured the hostname. Here's a review of the commands used.

```
S1#configure terminal
S1(config)#hostname S1
S1(config)#exit
```


Step 2. Set the access passwords.

Enter config-line mode for the console. Set the login password to **cisco**. Also configure the vty lines 0 to 15 with the password **cisco**.

```
S1#configure terminal
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

Why is the **login** command required? _____

Step 3. Set the command mode passwords.

Set the enable secret password to class.

```
S1(config)#enable secret class
```

Step 4. Configure the Layer 3 address of the switch.

Set the IP address of the switch to 172.17.99.11 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99. The VLAN must first be created on the switch before the address can be assigned.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

Step 5. Assign ports to the switch VLAN.

Assign Fastethernet 0/1, 0/8, and 0/18 to ports to VLAN 99.

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

Step 6. Set the switch default gateway.

S1 is a layer 2 switch, so it makes forwarding decisions based on the Layer 2 header. If multiple networks are connected to a switch, you need to specify how the switch forwards the internetwork frames, because the path must be determined at Layer three. This is done by specifying a default gateway address that points to a router or Layer 3 switch. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 172.17.99.1, set the default gateway for the switch.

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

Step 7. Verify the management LANs settings.

Verify the interface settings on VLAN 99 with the **show interface vlan 99** command.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
```



```
  Hardware is CPU Interface, address is 0060.47ac.1eb8 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
<Output Omitted>
```

What is the bandwidth on this interface? _____

What is the queuing strategy? _____

Step 8. Configure the IP address and default gateway for PC1.

Set the IP address of PC1 to 172.17.99.21, with a subnet mask of 255.255.255.0. Configure a default gateway of 172.17.99.11. Click PC1 and its Desktop tab then IP configuration to input the addressing parameters.

Step 9. Verify connectivity.

To verify the host and switch are correctly configured, ping the switch from PC1.

If the ping is not successful, troubleshoot the switch and host configuration. Note that this may take a couple of tries for the pings to succeed.

Step 10. Configure the port speed and duplex settings for a Fast Ethernet interface.

Configure the duplex and speed settings on Fast Ethernet 0/18. Use the **end** command to return to privileged EXEC mode when finished.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
```

The default on the Ethernet interface of the switch is auto-sensing, so it automatically negotiates optimal settings. You should set duplex and speed manually only if a port must operate at a certain speed and duplex mode. Manually configuring ports can lead to duplex mismatches, which can significantly degrade performance.

Notice how the link between PC1 and S1 went down. Remove the **speed 100** and **duplex full** commands. Now verify the settings on the Fast Ethernet interface with the **show interface fa0/18** command.

```
S1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
<Output omitted>
```


Step 11. Save the configuration.

You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made will not be lost if the system is rebooted or loses power.

```
S1#copy running-config startup-config

Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
S1#
```

Step 12. Examine the startup configuration file.

To see the configuration that is stored in NVRAM, issue the **show startup-config** command from privileged EXEC (enable mode).

Are all the changes that were entered recorded in the file?

Task 4: Managing the MAC Address Table

Step 1. Record the MAC addresses of the hosts.

Determine and record the Layer 2 (physical) addresses of the PC network interface cards using the following steps:

- Click the PC.
- Select the Desktop tab.
- Click Command Prompt.
- Type **ipconfig /all**

Step 2. Determine the MAC addresses that the switch has learned.

Display the MAC addresses using the **show mac-address-table** command in privileged EXEC mode. If there are no MAC addresses, ping from PC1 to S1 then check again.

```
S1#show mac-address-table
```

Step 3. Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac-address-table dynamic** command from privileged EXEC mode.

```
S1#clear mac-address-table dynamic
```

Step 4. Verify the results.

Verify that the MAC address table was cleared.

```
S1#show mac-address-table
```

Step 5. Examine the MAC table again.

Look at the MAC address table again in privileged EXEC mode. The table has not changed, ping S1 from PC1 and check again.

Step 6. Set up a static MAC address.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on Fast Ethernet interface 0/18 using the address that was recorded for PC1 in Step 1 of this task, 0002.16E8.C285.

```
S1(config)#mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
```

Step 7. Verify the results.

Verify the MAC address table entries.

```
S1#show mac-address-table
```

Step 8. Remove the static MAC entry.

Enter configuration mode and remove the static MAC by putting a **no** in front of the command string.

```
S1(config)#no mac-address-table static 0002.16E8.C285 vlan 99 interface
fastethernet 0/18
```

Step 9. Verify the results.

Verify that the static MAC address has been cleared with the **show mac-address-table static** command.

Task 5: Configuring Port Security

Step 1. Configure a second host.

A second host is needed for this task. Set the IP address of PC2 to 172.17.99.22, with a subnet mask of 255.255.255.0 and a default gateway of 172.17.99.11. Do not connect this PC to the switch yet.

Step 2. Verify connectivity.

Verify that PC1 and the switch are still correctly configured by pinging the VLAN 99 IP address of the switch from the host. If the pings were not successful, troubleshoot the host and switch configurations.

Step 3. Determine which MAC addresses that the switch has learned.

Display the learned MAC addresses using the **show mac-address-table** command in privileged EXEC mode.

Step 4. List the port security options.

Explore the options for setting port security on interface Fast Ethernet 0/18.

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
```

Step 5. Configure port security on an access port.

Configure switch port Fast Ethernet 0/18 to accept only two devices, to learn the MAC addresses of those devices dynamically, and to shutdown the port if a violation occurs.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation shutdown
```



```
S1(config-if)#exit
```

Step 6. Verify the results.

Show the port security settings with the **show port-security interface fa0/18** command.

How many secure addresses are allowed on Fast Ethernet 0/18?
What is the security action for this port?

Step 7. Examine the running configuration file.

```
S1#show running-config
```
Are there statements listed that directly reflect the security implementation of the running configuration?

Step 8. Modify the port security settings on a port.

On interface Fast Ethernet 0/18, change the port security maximum MAC address count to 1.

```
S1(config-if)#switchport port-security maximum 1
```

Step 9. Verify the results.

Show the port security settings with the **show port-security interface fa0/18** command.

Have the port security settings changed to reflect the modifications in Step 8?

Ping the VLAN 99 address of the switch from PC1 to verify connectivity and to refresh the MAC address table.

Step 10. Introduce a rogue host.

Disconnect the PC attached to Fast Ethernet 0/18 from the switch. Connect PC2, which has been given the IP address 172.17.99.22 to port Fast Ethernet 0/18. Ping the VLAN 99 address 172.17.99.11 from the new host.

What happened when you tried to ping S1?

Note: Convergence may take up to a minute. Switch between Simulation and Realtime mode to accelerate convergence.

Step 11. Reactivate the port.

As long as the rogue host is attached to Fast Ethernet 0/18, no traffic can pass between the host and switch. Reconnect PC1 to Fast Ethernet 0/18, and enter the following commands on the switch to reactivate the port:

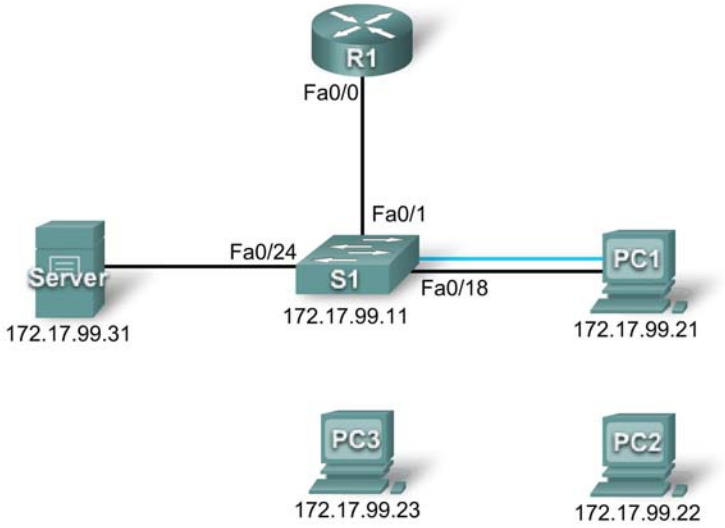
```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#no shutdown
S1(config-if)#exit
```

Step 12. Verify connectivity.

After convergence, PC1 should be able to again ping S1.

PT Activity 2.6.1: Packet Tracer Skills Integration Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	**Fa0/0**	172.17.99.1	255.255.255.0
S1	**Fa0/1**	172.17.99.11	255.255.255.0
PC1	**NIC**	172.17.99.21	255.255.255.0
PC2	**NIC**	172.17.99.22	255.255.255.0
Server	**NIC**	172.17.99.31	255.255.255.0

Objectives

- Establish console connection to switch
- Configure hostname and VLAN99
- Configure the clock
- Modify the history buffer
- Configure passwords and console/Telnet access
- Configure login banners
- Configure the router
- Configure the boot sequence
- Solve duplex and speed mismatch
- Manage the MAC address table

- Configure port security
- Secure unused ports
- Manage the switch configuration file

Introduction

In this Packet Tracer Skills Integration Challenge activity, you will configure basic switch management, including general maintenance commands, passwords, and port security. This activity provides you an opportunity to review previously acquired skills.

Task 1: Establish a Console Connection to a Switch

Step 1: Connect a console cable to S1.

For this activity, direct access to S1 Config and CLI tabs is disabled. You must establish a console session through PC1. Connect a console cable from PC1 to S1.

Step 2: Establish a terminal session.

From PC1, open a terminal window and use the default terminal configuration. You should now have access to the CLI for S1.

Step 3: Check results.

Your completion percentage should be 6%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure the Hostname and VLAN 99

Step 1: Configure the switch hostname as S1.

Step 2: Configure port Fa0/1 and interface VLAN 99.

Assign VLAN 99 to FastEthernet 0/1 and set the mode to access mode. These commands are discussed further in the next chapter.

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#switchport mode access
```

Configure IP connectivity on S1 using VLAN 99.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
```

Step 3: Configure the default gateway for S1.

Configure the default gateway and then test connectivity. S1 should be able to ping R1.

Step 4: Check results.

Your completion percentage should be 26%. If not, click **Check Results** to see which required components are not yet completed. Also, make sure that interface VLAN 99 is active.

Task 3: Configure the Clock Using Help

Step 1: Configure the clock to the current time.

At the privileged EXEC prompt, enter **clock ?**. Use Help to discover each additional step required to set the current time. Packet Tracer does not grade this command, so the completion percentage does not change.

Step 2: Verify that the clock is set to the current time.

Use the **show clock** command to verify that the clock is now set to the current time. Packet Tracer may not correctly simulate the time you entered.

Task 4: Modify the History Buffer

Step 1: Set the history buffer to 50 for the console line.

Step 2: Set the history buffer to 50 for the vty lines.

Step 3: Check results.

Your completion percentage should be 32%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure Passwords and Console/Telnet Access

Step 1: Configure the privileged EXEC password.

Use the encrypted form of the privileged EXEC mode password and set the password to **class**.

Step 2: Configure the passwords for console and Telnet.

Set the console and vty password to **cisco** and require users to log in.

Step 3: Encrypt passwords.

View the current configuration on S1. Notice that the line passwords are shown in clear text. Enter the command to encrypt these passwords.

Step 4: Check results.

Your completion percentage should be 41%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure the Login Banner

If you do not enter the banner text exactly as specified, Packet Tracer does not grade your command correctly. These commands are case-sensitive. Also make sure that you do not include any spaces before or after the text.

Step 1: Configure the message-of-the-day banner on S1.

Configure the message-of-the-day as **Authorized Access Only.**

Step 2: Check results.

Your completion percentage should be 44%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure the Router

Step 1: Configure the router with the same basic commands you used on S1.

Routers and switches share many of the same commands. Access the CLI for R1 by clicking the device. Do the following on R1:

- Configure the hostname
- Set the history buffer to 50 for both console and vty
- Configure the encrypted form of the privileged EXEC mode password and set the password to **class**
- Set the console and vty password to **cisco** and require users to log in
- Encrypt the console and vty passwords
- Configure the message-of-the-day as **Authorized Access Only**

Step 2: Check results.

Your completion percentage should be 65%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Configure the Boot Sequence

Step 1: View current files stored in flash.

On S1, enter the command **show flash**. You should see the following files listed:

```
S1#show flash
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    3  -rw-     4670455          <no date>  c2960-lanbase-mz.122-25.SEE1.bin
    2  -rw-         616          <no date>  vlan.dat

32514048 bytes total (23428056 bytes free)
```

Step 2: Configure S1 to boot using the second image listed.

Make sure your command includes the file system, which is **flash.**

Note: Packet Tracer does not show this command in the running configuration. In addition, if you reload the switch, Packet Tracer does not load the image you specified.

Step 3: Check results.

Your completion percentage should be 68%. If not, click **Check Results** to see which required components are not yet completed.

Task 9: Solve a Mismatch Between Duplex and Speed

Step 1: Change the duplex and speed on S1.

PC1 and Server currently do not have access through S1 because of a mismatch between duplex and speed. Enter commands on S1 to solve this problem.

Step 2: Verify connectivity.

Both PC1 and Server should now be able to ping S1, R1, and each other.

Step 3: Check results.

Your completion percentage should be 74%. If not, click **Check Results** to see which required components are not yet completed.

Task 10: Manage the MAC Address Table

Step 1: View the current MAC address table.

What command would you use to display the MAC address table?

```
S1#_____________________________________
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  99    0001.637b.b267    DYNAMIC     Fa0/24
  99    0004.9a32.8e01    DYNAMIC     Fa0/1
  99    0060.3ee6.1659    DYNAMIC     Fa0/18
```

The list of MAC address in your output may be different depending on how long it has been since you sent any packets across the switch.

Step 2: Configure a static MAC address.

Network policy may dictate that all server addresses be statically configured. Enter the command to statically configure the MAC address of Server.

Step 3: Check results.

Your completion percentage should be 76%. If not, click **Check Results** to see which required components are not yet completed.

Task 11: Configure Port Security

Step 1: Configure port security for PC1.

Use the following policy to establish port security on the port used by PC1:

- Enable port security
- Allow only one MAC address
- Configure the first learned MAC address to "stick" to the configuration
- Set the port to shut down if there is a security violation

Note: Only the enable port security step is graded by Packet Tracer and counted toward the completion percentage. However, all the port security tasks listed above are required to complete this activity successfully.

Step 2: Verify port security.

Verify that port security is enabled for Fa0/18. Your output should look like the following output. Notice that S1 has not yet learned a MAC address for this interface.

What command generated the following output?

```
S1#_____________________________________
Port Security              : Enabled
```



```
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Step 3: Force S1 to learn the MAC address for PC1.

Send a ping from PC1 to S1. Then verify that S1 has added the MAC address for PC1 to the running configuration.

```
!
interface FastEthernet0/18
 <output omitted>
 switchport port-security mac-address sticky 0060.3EE6.1659
 <output omitted>
!
```

Step 4: Test port security.

Remove the FastEthernet connection between S1 and PC1. Connect PC2 to Fa0/18. Wait for the link lights to turn green. If necessary, send a ping from PC2 to S1 to cause the port to shut down. Port security should show the following results:

```
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00D0.BAD6.5193:99
Security Violation Count   : 1
```

Viewing the Fa0/18 interface shows that **line protocol is down (err-disabled)**, which also indicates a security violation.

```
S1#show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
<output omitted>
```

Step 5: Reconnect PC1 and re-enable the port.

To re-enable the port, disconnect PC2 from Fa0/18 and reconnect PC1. Interface Fa0/18 must be manually configured before returning to the active state.

Step 6: Check results.

Your completion percentage should be 82%. If not, click **Check Results** to see which required components are not yet completed.

Task 12: Secure Unused Ports

Step 1: Disable all unused ports on S1.

Disable all ports that are currently not used on S1. Packet Tracer grades the status of the following ports: Fa0/2, Fa0/3, Fa0/4, Gig 1/1, and Gig 1/2.

Step 2: Check results.

Your completion percentage should be 97%. If not, click **Check Results** to see which required components are not yet completed.

Task 13: Manage the Switch Configuration File

Step 1: Save the current configuration to NVRAM for R1.

Step 2: Back up the startup configuration files for S1 and R1 to Server.

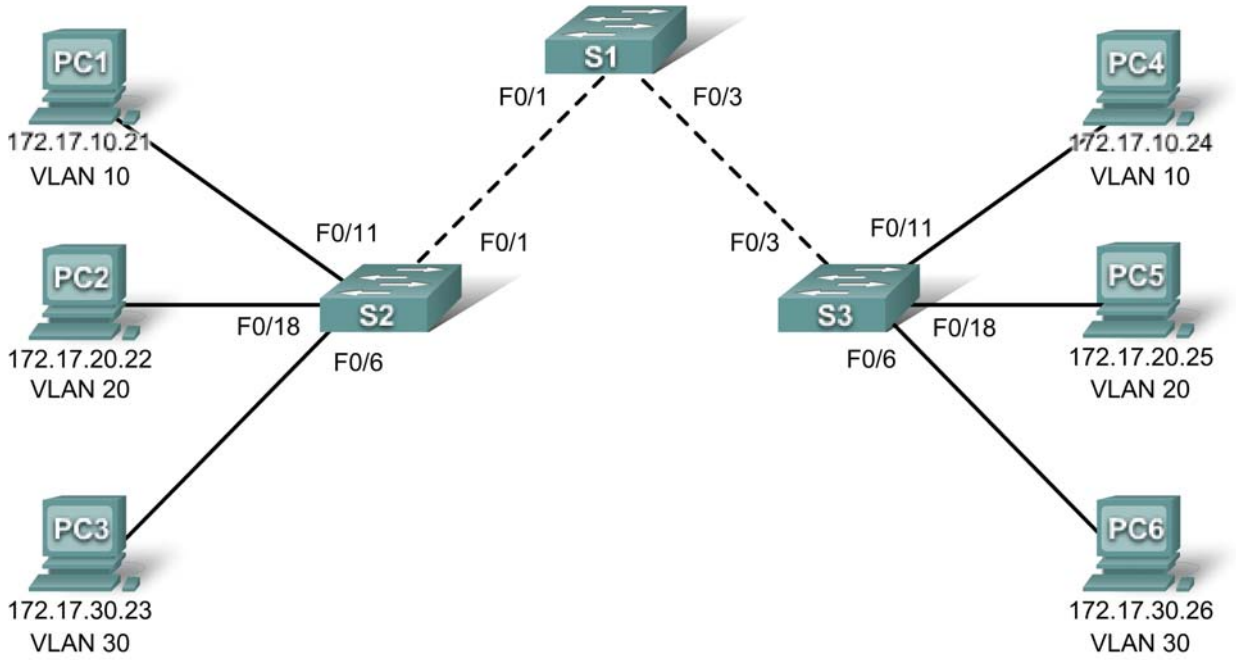
Back up the startup configuration file on S1 and R1 by uploading them to Server. Once complete, verify the server has the **R1-confg** and **S1-confg** files.

Step 3: Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 3.1.4: Investigating a VLAN Implementation

Topology Diagram



Learning Objectives

- Observe broadcast traffic in a VLAN implementation
- Observe broadcast traffic without VLANs

Introduction

This activity opens with completion at 100%. The purpose of the activity is to observe how broadcast traffic is forwarded by the switches when VLANs are configured and when VLANs are not configured.

Task 1: Observe Broadcast Traffic in a VLAN Implementation

Step 1: Ping from PC1 to PC6.

Wait for all the link lights to turn to green. To accelerate this process, switch back and forth between Simulation and Reatime mode.

Use the **Add Simple PDU** tool. Click PC1 and then PC6. Click the **Capture/Forward** button to step through the process. Observe the ARP requests as they traverse the network.

In normal operation, when a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports. Notice that S2 only sends the ARP request out Fa0/1 to S1. Also notice that S3 only sends the ARP request out Fa0/11 to PC4. PC1 and PC4 both belong to VLAN 10. PC6 belongs to VLAN 30. Because broadcast traffic is contained within the VLAN, PC6 never receives the ARP request from PC1. And because PC4 is not the destination, it discards the ARP request. The ping from PC1 fails, because PC1 never receives an ARP reply.

Step 2. Ping from PC1 to PC4.

Use the **Add Simple PDU** tool. Click PC1 and then PC4. Observe the ARP requests as they traverse the network. PC1 and PC4 both belong to VLAN 10, so the path of the ARP request is the same as before. Because PC4 is the destination, it replies to the ARP request. PC1 is then able to send the ping with the destination MAC address for PC4.

Task 2: Observe Broadcast Traffic without VLANs

Step 1. Clear the configurations on all three switches and delete the VLAN database.

On all three switches, enter user EXEC mode with the password **cisco**. Then enter privileged EXEC mode with the password **class**.

To observe broadcast traffic without VLANs, erase the configuration and delete the VLAN database on each switch. The commands for S1 are shown here.

```
S1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S1#delete vlan.dat
Delete filename [vlan.dat]? Enter
Delete flash:/vlan.dat? [confirm] Enter
```

Step 2. Reload the switches.

```
S1#reload
Proceed with reload? [confirm]Enter
```

Wait for all the link lights to return to green. To accelerate this process, switch back and forth between Simulation and Reatime mode.

Step 3. Click Capture/Forward to send ARP request and pings.

After the switches reload and the link lights return to green, the network is ready to forward your ARP and ping traffic. Click the **Capture/Forward** button to step through the process. Notice that the switches now forward the ARP requests out all ports, except the port on which the ARP request was received. This default action of switches is why VLANs can improve network performance. Broadcast traffic is contained within each VLAN.

Notice that the ping from PC1 to PC6 still fails. Why? What is required for this ping to succeed?

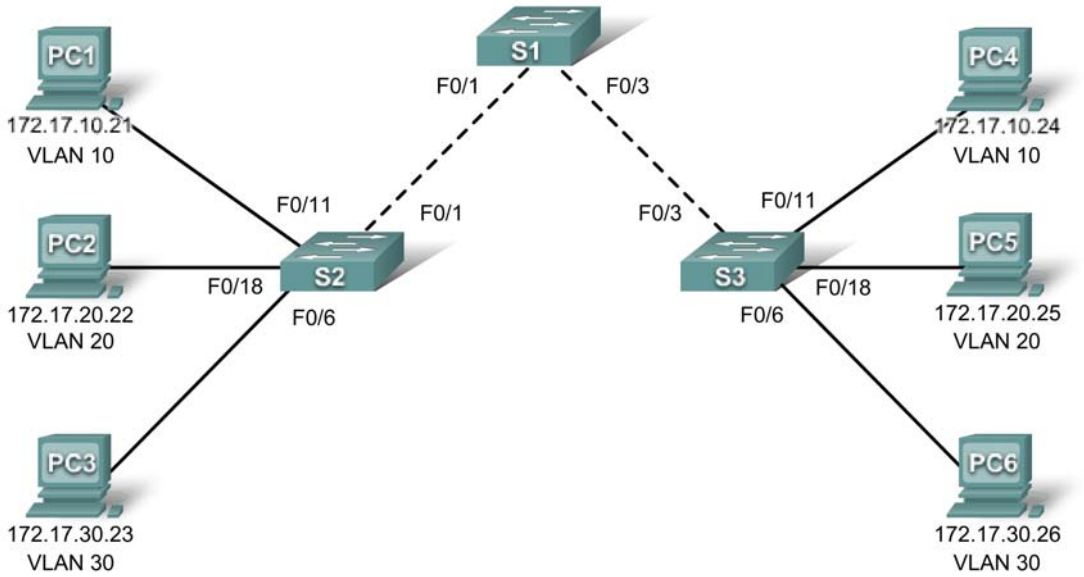
_____

_____

_____

PT Activity 3.2.3: Investigating VLAN Trunks

Topology Diagram



Learning Objectives

- Activate interface VLAN 99
- View the switch configuration
- Investigate the VLAN tag in the frame header

Introduction

Trunks carry the traffic of multiple VLANs through a single link, making them a vital part of communicating between switches with VLANs. This activity opens with completion at 100% and focuses on viewing switch configuration, trunk configuration, and VLAN tagging information.

Task 1: View the Switch Configuration

On S1, enter user EXEC mode with the password **cisco**. Then enter privileged EXEC mode with the password **class**. At the privileged EXEC prompt, issue the **show running-config** command.

```
S1#show running-config
```

Viewing the running configuration, note which interfaces are set to trunk. You will see the command **switchport mode trunk** under those interfaces.

Which interfaces are currently set to trunk?

_____

_____

The **switchport trunk native vlan 99** command is also listed under a number of interfaces. This command is used for setting the native VLAN for the trunk link. In this case, VLAN 99 is the native VLAN.

Task 2: Investigate the VLAN Tag in the Frame Header

Step 1. Ping from PC1 to PC4.

If link lights are still amber, switch back and forth between Realtime and Simulation mode until link lights turn green.

Use the **Add Simple PDU** tool. Click PC1 and then PC4.

Step 2. Click Capture/Forward to observe the ping.

Because PC1 and PC4 are on the same VLAN and Layer 3 network, PC4 sends back an ARP reply to PC1. PC1 then sends a ping to PC4. Finally, PC4 replies to the ping. Click **View Previous Events** when prompted.

Step 3. Investigate the PDU details at one of the switches.

Scroll to the top of the event list. Under the **Info** column, click the colored box for the event from S2 to S1. Then click the **Inbound PDU Details** tab. Notice the two fields that follow the source MAC address. What are the purposes of these two fields?

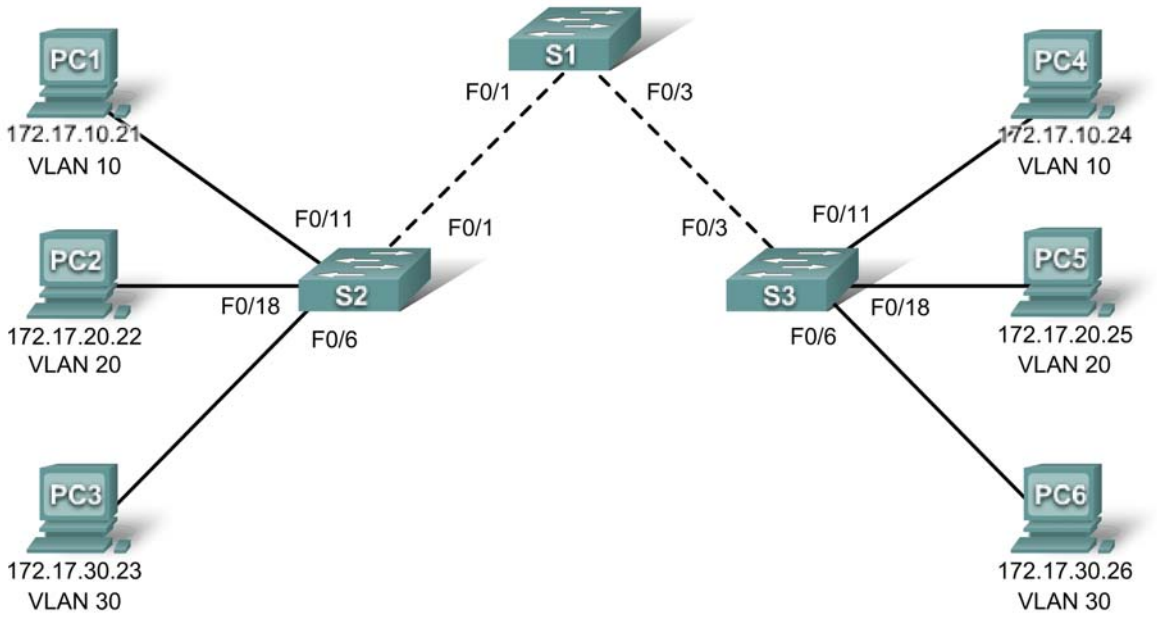
_____

_____

_____

PT Activity 3.3.4: Configuring VLANs and Trunks

Topology Diagram



Learning Objectives

- View the default VLAN configuration
- Configure VLANs
- Assign VLANs to ports
- Configure trunking

Introduction

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, assigning access ports to specific VLANs, changing the native VLAN, and configuring trunk links.

Task 1: View the Default VLAN Configuration

Step 1. Verify the current running configuration on the switches.

On all three switches, enter user EXEC mode with the password **cisco**. Then enter privileged EXEC mode with the password **class**.

From privileged EXEC mode on all three switches, issue the **show running-config** command to verify the current running configuration. The basic configurations are already set, but there are no VLAN assignments.

Step 2. Display the current VLANs.

On S1, issue the **show vlan** command. The only VLANs present are the default ones. By default, all interfaces are assigned to VLAN 1.

Step 3. Verify connectivity between PCs on the same network.

Notice that each PC can ping the other PC that shares the same network:

- PC1 can ping PC4
- PC2 can ping PC5
- PC3 can ping PC6

Pings to PCs in other networks fail.

What benefit will configuring VLANs provide to the current configuration?

_____

_____

_____

Task 2: Configure VLANs

Step 1. Create VLANs on S1.

The command **vlan** *vlan-id* creates a VLAN. Use the **name** *vlan-name* command to name a VLAN.

On S1, create four VLANs using the *vlan-ids* and the names shown below:

```
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name Students
S1(config-vlan)#vlan 30
S1(config-vlan)#name Guest(Default)
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management&Native
```

Step 2. Verify the VLAN configuration.

After creating the VLANs, return to privileged EXEC and issue the **show vlan brief** command to verify the creation of the new VLANs.

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```


Step 3. Create the VLANs on S2 and S3.

On S2 and S3, use the same commands you used on S1 to create and name the VLANs.

Step 4. Verify the VLAN configuration.

Use the **show vlan brief** command to verify all VLANs are configured and named.

Step 5. Check results.

Your completion percentage should be 38%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Assign VLANs to Ports

The **range** command greatly reduces the amount of repetitive commands you must enter when configuring the same commands on multiple ports. However, Packet Tracer does not support the **range** command. So only the active interfaces are graded for the **switchport mode access** command.

Step 1. Assign VLANs to the active ports on S2.

The **switchport mode access** command configures the interface as an access port. The **switchport access vlan** *vlan-id* command assigns a VLAN to the port. An access port can only be assigned one access VLAN. Enter the following commands on S2.

```
S2(config)#interface fastEthernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fastEthernet 0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fastEthernet 0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
```

Step 2. Assign VLANs to the active ports on S3.

Assign VLANs to the active ports on S3. S3 uses the same VLAN access port assignments that you configured on S2.

Step 3. Verify loss of connectivity.

Previously, PCs that shared the same network could ping each other successfully. Try pinging between PC1 and PC4. Although the access ports are assigned to the appropriate VLANs, the ping fails. Why?

_____

_____

_____

Step 4. Check results.

Your completion percentage should be 75%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure Trunking

Step 1. Configure S1 Fa0/1 and Fa0/3 for trunking and to use VLAN 99 as the native VLAN.

```
S1(config)#interface FastEthernet 0/1
```



```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#interface FastEthernet 0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
```

The trunk port takes about a minute to become active again. You can switch between Realtime and Simulation modes three or four times to quickly bring the port back up.

Then, the ports on S2 and S3 that connect to S1 become inactive. Again, switch between Realtime and Simulation modes three or four times to quickly bring the ports back up.

Once the ports become active, you periodically receive the following syslog messages:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (99), with S2 FastEthernet0/1 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/3 (99), with S3 FastEthernet0/3 (1).
```

You configured the native VLAN on S1 to be VLAN 99. However, the native VLAN on S2 and S3 is set to the default VLAN 1.

Step 2. Verify connectivity between devices on the same VLAN.

Although there is currently a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Why?

_____

_____

_____

Step 3. Verify trunking is enabled on S2 and configure VLAN 99 as the native VLAN.

Dynamic Trunking Protocol (DTP) has automatically enabled the Fast Ethernet 0/1 port on S2 for trunking. Once you configured the mode to trunking on S1, DTP messages sent from S1 to S2 automatically informed S1 to move the state of Fa0/1 to trunking. This can be verified with the following command on S1:

```
S2#show interface fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
S2#
```

Notice that the administrative mode is set to **dynamic auto**. This is the default state of all ports on a Cisco IOS switch. However, DTP has negotiated trunking, so the operation mode is **trunk**, resulting in a native VLAN mismatch.

As a best practice, configure the administrative mode of the trunking interface to be in trunk mode. This ensures that the interface is statically configured as a trunk port and never negotiates a different mode.

```
S2(config)#interface FastEthernet 0/1
S2(config-if)#switchport mode trunk
```


To correct the native VLAN mismatch, configure the trunking port with the **switchport trunk native vlan 99** command.

```
S2(config-if)#switchport trunk native vlan 99
```

Step 4. Verify trunking is enabled on S3 and configure VLAN 99 as the native VLAN.

DTP has also successfully negotiated a trunk between S1 and S3.

```
S3#show interfaces fastEthernet 0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
S3#
```

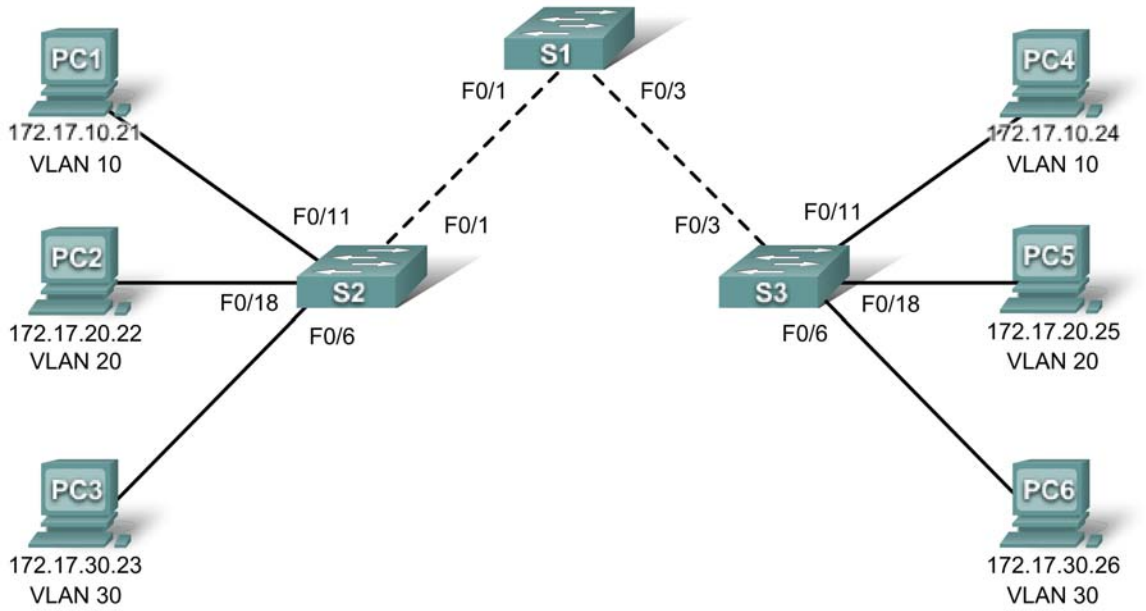
Configure the administrative mode of the trunking interface to be in trunk mode, and correct the native VLAN mismatch with the **switchport trunk native vlan 99** command.

Step 4. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 3.4.2: Troubleshooting a VLAN Implementation

Topology Diagram



Addressing Table

Device	IP Address	Subnet Mask	Default Gateway
PC1	172.17.10.21	255.255.255.0	172.17.10.1
PC2	172.17.20.22	255.255.255.0	172.17.20.1
PC3	172.17.30.23	255.255.255.0	172.17.30.1
PC4	172.17.10.24	255.255.255.0	172.17.10.1
PC5	172.17.20.25	255.255.255.0	172.17.20.1
PC6	172.17.30.26	255.255.255.0	172.17.30.1

Learning Objectives

- Test connectivity
- Investigate connectivity problems by gathering data
- Implement the solution and test connectivity

Introduction

In this activity, you will troubleshoot connectivity problems between PCs on the same VLAN. The activity is complete when you achieve 100% and the PCs can ping the other PCs on the same VLAN. Any solution you implement must conform to the topology diagram.

Task 1: Test Connectivity between PCs on the same VLAN

Use the **Add Simple PDU** tool to ping between two PCs on the same VLAN. The following tests should be successful at the conclusion of this activity. However, these tests will fail at this point.

- PC1 cannot ping PC4
- PC2 cannot ping PC5
- PC3 cannot ping PC6

Task 2: Gather Data on the Problem

Step 1. Verify the configuration on the PCs.

Are the following configurations for each PC correct?

- IP address
- Subnet mask
- Default gateway

Step 2. Verify the configuration on the switches.

Are the configurations on the switches correct? Be sure to verify the following:

- Ports assigned to the correct VLANs
- Ports configured for the correct mode
- Ports connected to the correct device

Step 3: Document the problem and suggest solutions.

What are the reasons why connectivity failed between the PCs? What are the solutions? There could be more than one problem and more than one solution. All solutions must conform to the topology diagram.

PC1 to PC4

Problem: _____

Solution: _____

PC2 to PC5

Problem: _____

Solution: _____

PC3 to PC6

Problem: _____

Solution: _____

Task 3: Implement the Solution and Test Connectivity

Step 1: Make changes according to the suggested solutions in Task 2.

Step 2: Test connectivity between PCs on the same VLAN.

If you change any IP configurations, you should create new pings, because the prior pings use the old IP address.

- PC1 should be able to ping PC4
- PC2 should be able to ping PC5
- PC3 should be able to ping PC6

Can PC1 ping PC4? _____

Can PC2 ping PC5? _____

Can PC3 ping PC6? _____

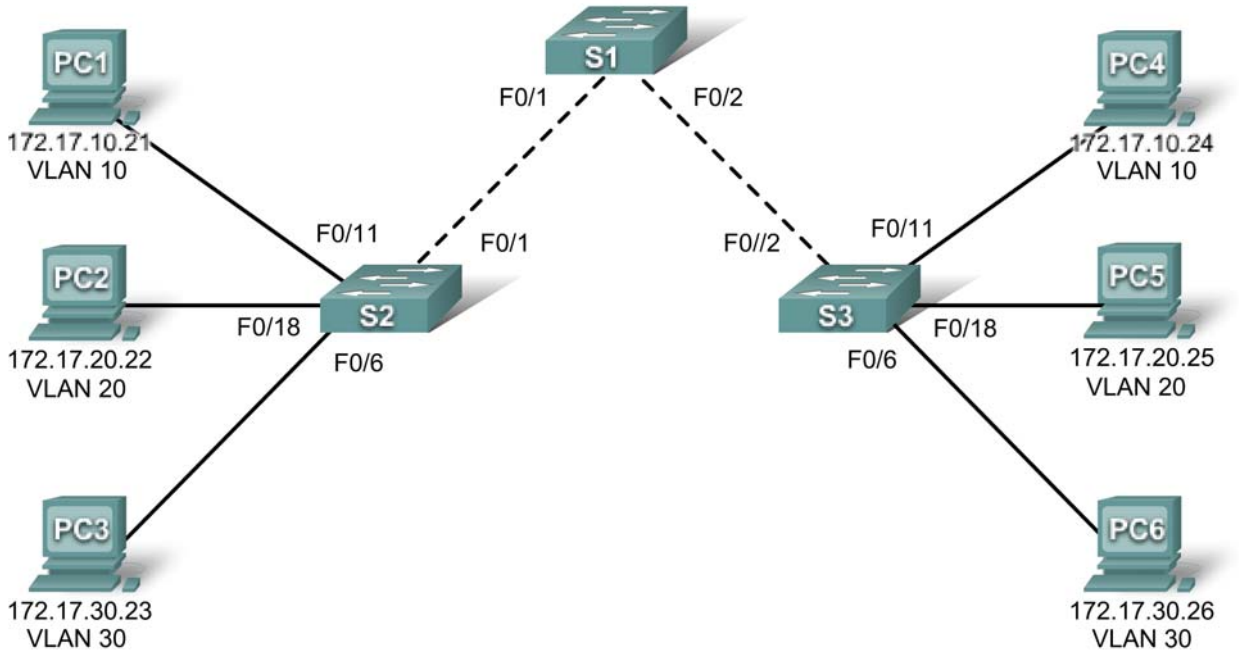
If any pings fail, return to Task 2 to continue troubleshooting.

Step 3. Check completion percentage.

Your completion percentage should be 100%. If not, return to Step 1 and continue to implement your suggested solutions. You will not be able to click **Check Results** and see which required components are not yet completed

PT Activity 3.5.1: Basic VLAN Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.11	255.255.255.0	N/A
S2	**VLAN 99**	172.17.99.12	255.255.255.0	N/A
S3	**VLAN 99**	172.17.99.13	255.255.255.0	N/A
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**NIC**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**NIC**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**NIC**	172.17.30.26	255.255.255.0	172.17.30.1

Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	VLAN 99 – Management&Native	172.17.99.0/24
Fa0/6 – 0/10	VLAN 30 – Guest(Default)	172.17.30.0/24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0/24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0/24

Learning Objectives

- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Task 1: Perform Basic Switch Configurations

Perform Basic Switch Configurations. Packet Tracer will only grade switch hostnames.

- Configure the switch hostnames.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Task 2: Configure and Activate Ethernet Interfaces

Configure the Ethernet interfaces of the six PCs with the IP addresses and default gateways from the addressing table.

Note: The IP address for PC1 will be marked as wrong for now. You will change the PC1 IP address later.

Task 3: Configure VLANs on the Switch

Step 1. Create VLANs on switch S1.

Use the **vlan** *vlan-id* command in global configuration mode to add VLANs to switch S1. There are four VLANs to configure for this activity. After you create the VLAN, you will be in vlan configuration mode, where you can assign a name to the VLAN with the **vlan** *name* command.

```
S1(config)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
```



```
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name Students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name Guest(Default)
S1(config-vlan)#exit
```

Step 2. Verify that the VLANs have been created on S1.

Use the **show vlan brief** command to verify that the VLANs have been created.

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
```

Step 3. Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20, 30, and 99 on S2 and S3 using the commands from Step 1. Verify the correct configuration with the **show vlan brief** command.

What ports are currently assigned to the four VLANs you have created?

_____

Step 4. Assign switch ports to VLANs on S2 and S3.

Refer to the port assignment table. Ports are assigned to VLANs in interface configuration mode, using the **switchport access vlan** *vlan-id* command. Packet Tracer will only grade the first interface in each range (the interface the PC is connected to). Normally you would use the **interface range** command, but Packet Tracer does not support this command.

```
S2(config)#interface fastEthernet0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fastEthernet0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fastEthernet0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Note: The Fa0/11 access VLAN will be marked as wrong for now. You will correct this later in the activity.

Repeat the same commands on S3.

Step 5. Determine which ports have been added.

Use the **show vlan id** *vlan-number* command on S2 to see which ports are assigned to VLAN 10.

Which ports are assigned to VLAN 10? _____

Note: The **show vlan name** *vlan-name* displays the same output.

You can also view VLAN assignment information using the **show interfaces switchport** command.

Step 6. Assign the management VLAN.

A management VLAN is any VLAN that you configure to access the management capabilities of a switch. VLAN 1 serves as the management VLAN if you did not specifically define another VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 is a bad choice as the management VLAN. You do not want an arbitrary user who is connecting to a switch to default to the management VLAN. Recall that you configured the management VLAN as VLAN 99 earlier in this lab.

From interface configuration mode, use the **ip address** command to assign the management IP address to the switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Assigning a management address allows IP communication between the switches, and also allows any host connected to a port assigned to VLAN 99 to connect to the switches. Because VLAN 99 is configured as the management VLAN, any ports assigned to this VLAN are considered management ports and should be secured to control which devices can connect to these ports.

Step 7. Configure trunking and the native VLAN for the trunking ports on all switches.

Trunks are connections between the switches that allow the switches to exchange information for all VLANS. By default, a trunk port belongs to all VLANs, as opposed to an access port, which can only belong to a single VLAN. If the switch supports both ISL and 802.1Q VLAN encapsulation, the trunks must specify which method is being used. Because the 2960 switch only supports 802.1Q trunking, it is not specified in this activity.

A native VLAN is assigned to an 802.1Q trunk port. In the topology, the native VLAN is VLAN 99. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. One of the IEEE 802.1Q specifications for Native VLANs is to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For the purposes of this activity, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#interface fa0/2
```



```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#end

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#end

S3(config)#interface fa0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#end
```

Verify that the trunks have been configured with the show interface trunk command.

```
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,99,1002,1003,1004,1005
Fa0/2       1,10,20,30,99,1002,1003,1004,1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,99,1002,1003,1004,1005
Fa0/2       1,10,20,30,99,1002,1003,1004,1005
```

Step 8. Verify that the switches can communicate.

From S1, ping the management address on both S2 and S3.

```
S1#ping 172.17.99.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
..!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

S1#ping 172.17.99.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
..!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Step 9. Ping several hosts from PC2.

Ping from host PC2 to host PC1 (172.17.10.21). Is the ping attempt successful? _____

Ping from host PC2 to the switch VLAN 99 IP address 172.17.99.12. Is the ping attempt successful?

_____

Because these hosts are on different subnets and in different VLANS, they cannot communicate without a Layer 3 device to route between the separate subnetworks.

Ping from host PC2 to host PC5. Is the ping attempt successful? _____

Because PC2 is in the same VLAN and the same subnet as PC5, the ping is successful.

Step 10. Move PC1 into the same VLAN as PC2.

The port connected to PC2 (S2 Fa0/18) is assigned to VLAN 20, and the port connected to PC1 (S2 Fa0/11) is assigned to VLAN 10. Reassign the S2 Fa0/11 port to VLAN 20. You do not need to first remove a port from a VLAN to change its VLAN membership. After you reassign a port to a new VLAN, that port is automatically removed from its previous VLAN.

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface fastethernet 0/11
S2(config-if)#switchport access vlan 20
S2(config-if)#end
```

Ping from host PC2 to host PC1. Is the ping attempt successful? _____

Step 11. Change the IP address and network on PC1.

Change the IP address on PC1 to 172.17.20.21. The subnet mask and default gateway can remain the same. Once again, ping from host PC2 to host PC1, using the newly assigned IP address.

Is the ping attempt successful? _____

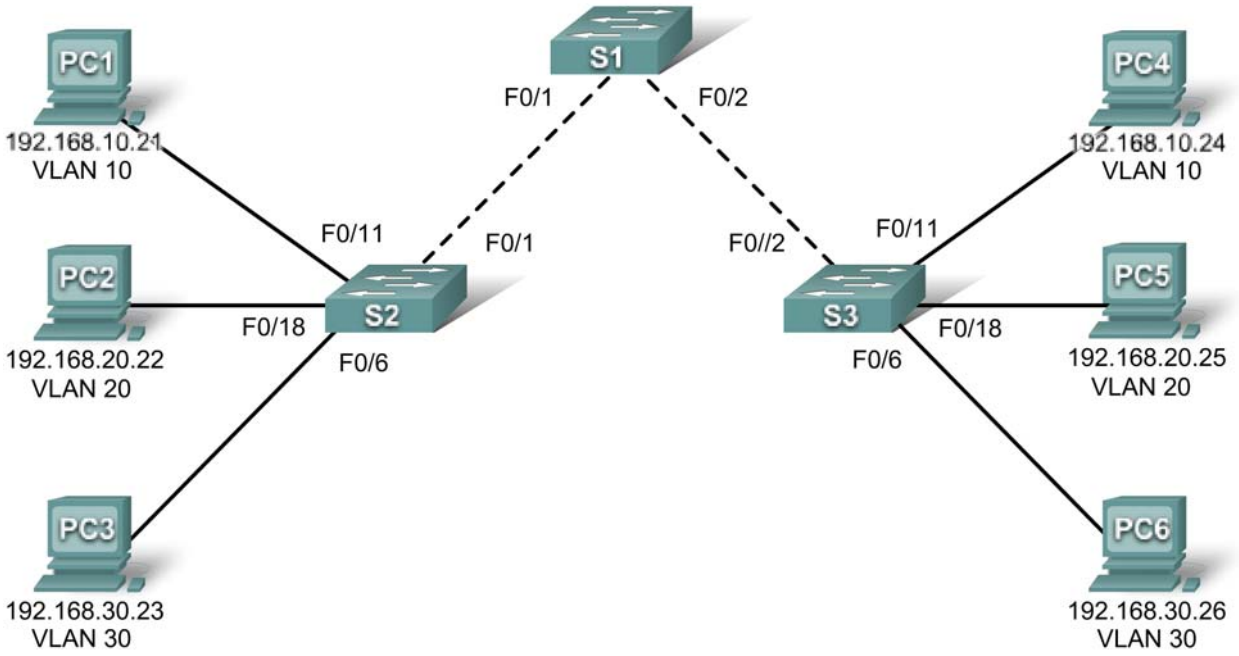
Why was this attempt successful?

_____

_____

PT Activity 3.5.2: Challenge VLAN Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 56**	192.168.56.11	255.255.255.0	N/A
S2	**VLAN 56**	192.168.56.12	255.255.255.0	N/A
S3	**VLAN 56**	192.168.56.13	255.255.255.0	N/A
PC1	**NIC**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**NIC**	192.168.20.23	255.255.255.0	192.168.30.1
PC4	**NIC**	192.168.10.24	255.255.255.0	192.168.10.1
PC5	**NIC**	192.168.20.25	255.255.255.0	192.168.20.1
PC6	**NIC**	192.168.30.26	255.255.255.0	192.168.30.1

Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	VLAN 99 – Management&Native	192.168.56.0/24
Fa0/6 – 0/10	VLAN 30 – Guest(Default)	192.168.30.0/24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0/24
Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0/24

Learning Objectives

- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Task 1: Perform Basic Switch Configurations

Configure the switches according to the following guidelines. Packet Tracer will only grade hostnames.

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Task 2: Configure and Activate Ethernet Interfaces

Step 1. Configure the PCs.

Configure the Ethernet interfaces of the six PCs with the IP addresses and default gateways from the addressing table at the beginning of the activity. The IP address for PC1 will be graded as incorrect for now. You will change the PC1 address later in the activity.

Step 2. Enable the user ports for access on S2 and S3.

Task 3: Configure VLANs on the Switch

Step 1. Create VLANs on switch S1.

The VLAN IDs and names are listed in the Port Assignments table at the beginning of this activity.

Step 2. Verify that the VLANs have been created on S1.

Step 3. Configure, name, and verify VLANs on switches S2 and S3.

Step 4. Assign switch ports to VLANs on S2 and S3.

Note: The S2 Fa0/11 port will be graded incorrect for now and Packet Tracer will only grade the first port assignment for each VLAN.

Step 5. Determine which ports have been added to VLAN 10 on S2.

Step 6. Configure management VLAN 56 on each of the switches.

Step 7. Configure trunking and the native VLAN for the trunking ports on all three switches. Verify that the trunks have been configured.

Step 8. Verify that S1, S2, and S3 can communicate.

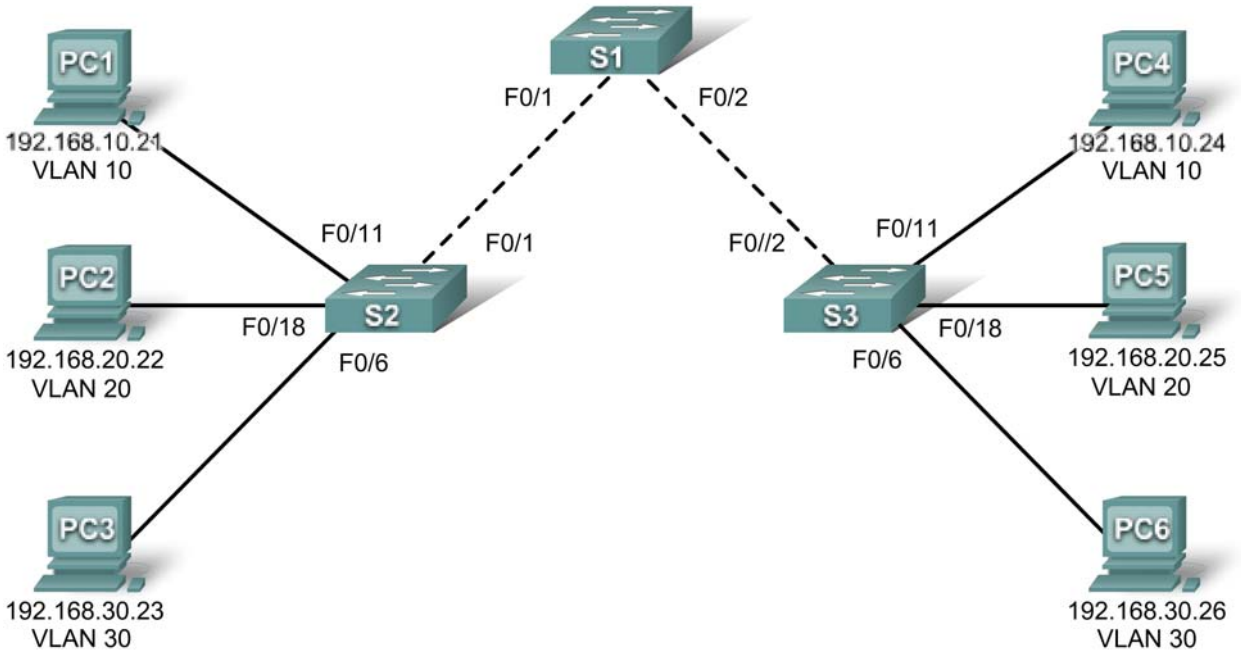
Step 9. Ping several hosts from PC2. What is the result?

Step 10. Move PC1 into the same VLAN as PC2. Can PC1 successfully ping PC2?

Step 11. Change the IP address on PC1 to 192.168.20.21. Can PC1 successfully ping PC2?

PT Activity 3.5.3: Troubleshooting VLAN Configurations

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 56**	192.168.56.11	255.255.255.0	N/A
S2	**VLAN 56**	192.168.56.12	255.255.255.0	N/A
S3	**VLAN 56**	192.168.56.13	255.255.255.0	N/A
PC1	**NIC**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**NIC**	192.168.20.23	255.255.255.0	192.168.30.1
PC4	**NIC**	192.168.10.24	255.255.255.0	192.168.10.1
PC5	**NIC**	192.168.20.25	255.255.255.0	192.168.20.1
PC6	**NIC**	192.168.30.26	255.255.255.0	192.168.30.1

Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	VLAN 56 – Management&Native	192.168.56.0/24
Fa0/6 – 0/10	VLAN 30 – Guest(Default)	192.168.30.0/24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0/24
Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0/24

Learning Objectives

- Find and Correct Network Errors
- Document the Corrected Network

Introduction

In this activity, you will practice troubleshooting a misconfigured VLAN environment. The initial network has errors. Your objective is to locate and correct any and all errors in the configurations and establish end-to-end connectivity. Your final configuration should match the topology diagram and addressing table. All passwords are set to **cisco**, except the **enable secret** password, which is set to **class**.

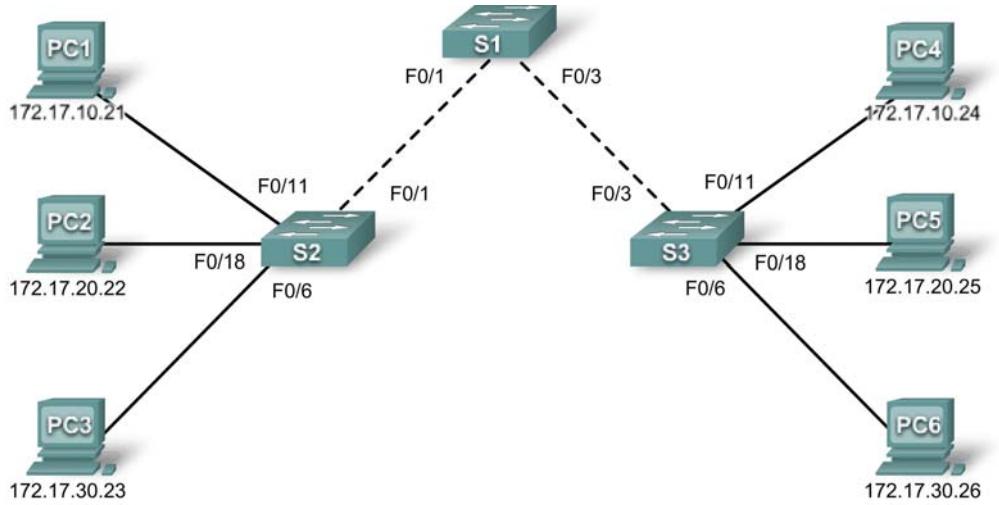
Task 1: Find and Correct Network Errors

Once all errors are corrected, PCs belonging to the same VLAN should be able to ping each other. In addition, S1, S2, and S3 should be able to ping each other.

Task 2: Document the Corrected Network

PT Activity 3.6.1: Packet Tracer Skills Integration Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.31	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.32	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.33	255.255.255.0	172.17.99.1
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**NIC**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**NIC**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**NIC**	172.17.30.26	255.255.255.0	172.17.30.1

Learning Objectives

- Add and connect switches
- Add and connect PCs
- Verify basic device configuration and connectivity
- Configure and verify port security
- Configure VLANs on the switches
- Configure trunks on the switches
- Verify end-to-end connectivity

Introduction

In this activity, you will connect and completely configure the Chapter 3 topology, including adding and connecting devices, and configuring security and VLANs.

Task 1: Add and Connect the Switches

Step 1. Add the S2 switch.

S2 must be a 2960 series switch. Change the display name and hostname to S2. Names are case-sensitive.

Step 2. Connect S2 to S1.

Connect S2 Fa0/1 to S1 Fa0/1.

Step 3. Add the S3 switch.

S3 must be a 2960 series switch. Change the display name and hostname to S3. Names are case-sensitive.

Step 4. Connect S3 to S1.

Connect S3 Fa0/3 to S1 Fa0/3.

Step 5. Check results.

Your completion percentage should be 9%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Add and Connect the PCs

Step 1. Add PC1, PC2, PC3, PC4, PC5, and PC6.

- Add the six PCs according to the chapter topology.
- If necessary, change the display name to match the names in the addressing table. Display names are case-sensitive.

Step 2. Connect PC1, PC2, and PC3 to S2.

- Connect PC1 to Fa0/11 on S2
- Connect PC2 to Fa0/18 on S2
- Connect PC3 to Fa0/6 on S2

Step 3. Connect PC4, PC5, and PC6 to S3.

- Connect PC4 to Fa0/11 on S3
- Connect PC5 to Fa0/18 on S3
- Connect PC6 to Fa0/6 on S3

Step 4. Check results.

Your completion percentage should be 29%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Devices and Verify Connectivity

Step 1. Configure switches with basic commands.

Configure each switch with the following basic settings. Packet Tracer only grades the **hostname** command.

- Hostname on S1
- Banner
- Enable secret password
- Line configurations
- Service encryption

Step 2. Configure the management VLAN interface on S1, S2, and S3.

Configure VLAN 99 as the management VLAN interface on S1, S2, and S3. This interface is not active until after trunking is configured later in the activity. However, activate the interface at this time with the appropriate command.

Step 3. Configure PC IP addressing.

Configure the PCs with IP addressing according to the addressing table.

Step 4. Verify that PCs on the same subnet can ping each other.

Use the **Add Simple PDU tool to create** pings between PCs on the same VLAN. Verify that the following PCs can ping each other:

- PC1 to PC4
- PC2 to PC5
- PC3 to PC6

Step 5. In simulation mode, observe the broadcast traffic.

- Clear the learned MAC addresses so that the switches must broadcast ping packets.
- In simulation mode, observe the broadcast traffic that propagates throughout the LAN until the switches learn the ports of each PC.

Step 6. Check results.

Your completion percentage should be 53%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure and Verify Port Security

Step 1. Configure access links with port security.

Normally, you configure port security on all access ports or shut down the port if it is not in use. Use the following policy to establish port security just on the ports used by the PCs.

- Set the port to access mode.
- Enable port security.
- Allow only one MAC address.
- Configure the first learned MAC address to “stick” to the configuration.
- Set the port to shut down if there is a security violation.

Force the switches to learn the MAC addresses by sending pings across all three switches

Note: Only enabling port security is graded by Packet Tracer. However, all the port security tasks listed above are required to complete this activity.

Step 2. Verify port security is active for the interfaces attached to PCs.

What command would you use to verify that port security is active on an interface?

_____

```
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.0F00.6668:1
Security Violation Count   : 0
```

Note: The **Last Source Address:Vlan** information should show a MAC address. Your MAC address may be different than the one shown here. If the MAC address in this field is 0000.0000.0000, send traffic to the port by pinging across the switch to the other PC on the same subnet.

Step 3. Test port security.

- Connect PC2 to the port of PC3, and connect PC3 to the port of PC2.
- Send pings between PCs on the same subnet.
- The ports for PC2 and PC3 should shut down.

Step 4. Verify that ports are err-disabled and that a security violation has been logged.

What command shows the following output?

_____

```
FastEthernet0/6 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 000a.41e8.c906 (bia 000a.41e8.c906)
<output omitted>
```

What command shows the following output?

_____

```
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.0F00.6668:1
Security Violation Count   : 1
```


Step 5. Reconnect PCs to the correct port and clear port security violations.

- Connect PC2 and PC3 back to the correct port.
- Clear the port security violation.
- Verify that PC2 and PC3 can send pings across S2.

Step 6. Check results.

Your completion percentage should be 75%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure VLANs on the Switches

Step 1. Create and name the VLANs.

Create and name the following VLANs on the switches S1, S2, and S3:

- VLAN 10, name = **Faculty/Staff**
- VLAN 20, name = **Students**
- VLAN 30, name = **Guest(Default)**
- VLAN 99, name = **Management&Native**

Step 2. Assign access ports to the VLANs.

Assign the following PC access ports to the VLANs:

- VLAN 10: PC1 and PC4
- VLAN 20: PC2 and PC5
- VLAN 30: PC3 and PC6

Step 3. Verify VLAN implementation.

What command verifies the VLAN configuration, including the port assignments?

_____

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig1/1, Gig1/2
10   Faculty/Staff                     active    Fa0/11
20   Students                          active    Fa0/18
30   Guest(Default)                    active    Fa0/6
99   Management&Native                 active
<output omitted>
```

Step 4. Check results.

Your completion percentage should be 92%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure Trunks on the Switches

Step 1. Configure trunking on the appropriate interfaces.

- Configure trunking on the appropriate interfaces on switch S1.
- Verify that switches S2 and S3 are now in trunking mode.
- Manually configure the appropriate interfaces on S2 and S3 for trunking.
- Configure VLAN 99 as the native VLAN for all trunks.

Step 2. Test connectivity

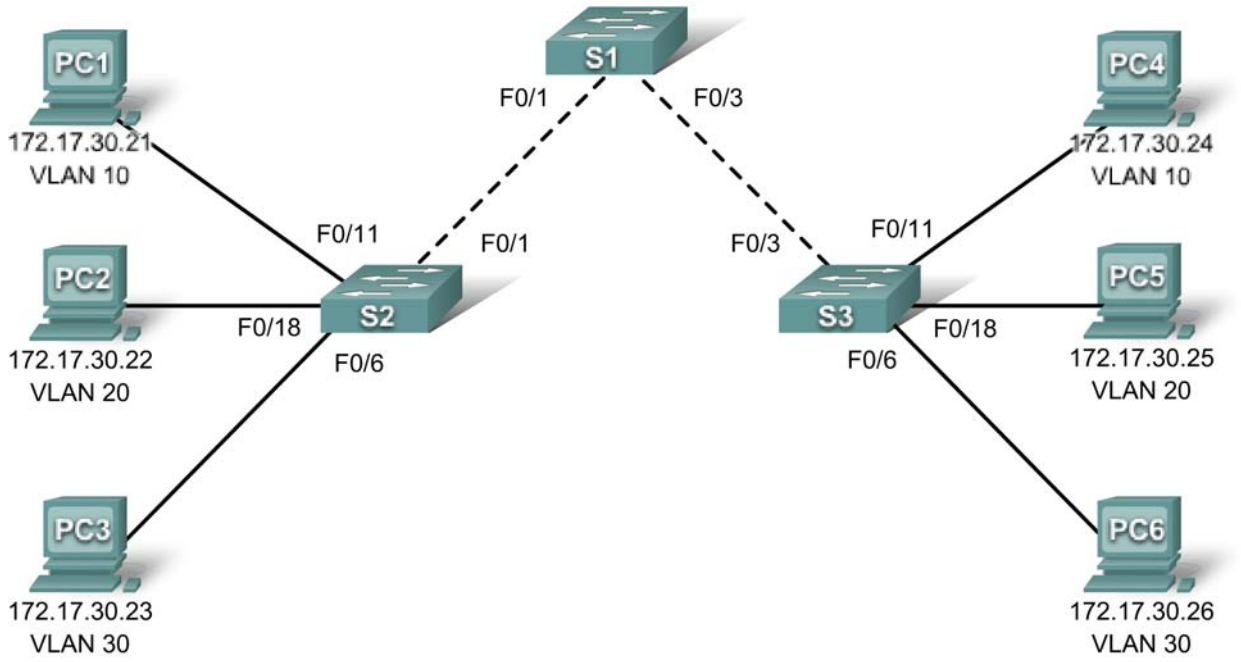
After the switch trunk ports transition to the forwarding state (green link lights), you should be able to successfully ping between PCs on the same VLAN.

Step 3. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 4.3.3: Configure VTP

Topology Diagram



Learning Objectives

- Investigate the current configuration
- Configure S1 as VTP server
- Configure S2 and S3 as VTP clients
- Configure VLANs on S1
- Configure trunks on S1, S2, and S3
- Verify VTP status on S1, S2, and S3
- Assign VLANs to ports on S2 and S3
- Verify VLAN implementation and test connectivity

Introduction

In this activity, you will practice configuring VTP. When Packet Tracer first opens, the switches already contain a partial configuration. The user EXEC password is **cisco** and the privileged EXEC password is **class**.

Task 1: Investigate the Current Configuration

Step 1. Verify the current running configuration on the switches.

What configurations are already present on the switches?

_____

_____

_____

Step 2. Display the current VLANs on each switch.

Are there any VLANs present? Are the VLANs user created VLANs or default VLANs?

_____

```
S1#show vlan brief
VLAN Name                         Status    Ports
---- ------------------------ --------- -------------------------------
1    default                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                            Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                            Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                            Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                            Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                            Gig1/1, Gig1/2
1002 fddi-default                 active
1003 token-ring-default           active
1004 fddinet-default              active
1005 trnet-default                active
```

Completion should be at 0% at the end of this Task.

Task 2: Configure S1 as VTP Server

Step 1. Configure the VTP mode command.

S1 will be the server for VTP. Set S1 to server mode.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#
```

Notice that the switch is already set to server mode by default. However, it is important that you explicitly configure this command to insure the switch is in server mode.

Step 2. Configure the VTP domain name.

Configure S1 with **CCNA** as the VTP domain name. Remember that VTP domain names are case sensitive.

```
S1(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
```

Step 3. Configure the VTP domain password.

Configure S1 with **cisco** as the VTP domain password. Remember that VTP domain passwords are case sensitive.

```
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#
```


Step 4. Confirm configuration changes.

Use the **show vtp status** command on S1 to confirm that the VTP mode and domain are configured correctly.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

To verify the VTP password, use the **show vtp password** command.

```
S1#show vtp password
VTP Password: cisco
S1#
```

Step 5. Check results.

Your completion percentage should be 8%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure S2 and S3 as VTP Clients

Step 1. Configure the VTP mode command.

S2 and S3 will be VTP clients. Set these two switches to client mode.

Step 2. Configure the VTP domain name.

Before S2 and S3 will accept VTP advertisements from S1, they must belong to the same VTP domain. Configure S2 and S3 with **CCNA** as the VTP domain name. Remember that VTP domain names are case sensitive.

Step 3. Configure the VTP domain password.

S2 and S3 must also use the same password before they can accept VTP advertisements from the VTP server. Configure S2 and S3 with **cisco** as the VTP domain password. Remember that VTP domain passwords are case sensitive.

Step 4. Confirm configuration changes.

Use the **show vtp status** command on each switch to confirm that the VTP mode and domain are configured correctly. Output for S3 is shown here.

```
S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Client
```



```
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Notice that the configuration revision number is 0 on all three switches. Why?

_____

_____

_____

To verify the VTP password, use the **show vtp password** command.

```
S3#show vtp password
VTP Password: cisco
S3#
```

Step 5. Check results.

Your completion percentage should be 31%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure VLANs on S1

VLANs can be created on the VTP server and distributed to other switches in the VTP domain. In this task you will create 4 new VLANs on the VTP server, S1. These VLANs will be distributed to S2 and S3 via VTP.

Step 1. Create the VLANs.

For grading purposes in Packet Tracer, the VLAN names are case-sensitive.

- VLAN 10 named **Faculty/Staff**
- VLAN 20 named **Students**
- VLAN 30 named **Guest(Default)**
- VLAN 99 named **Management&Native**

Step 2. Verify VLANs.

Use the **show vlan brief** command to verify the VLANs and their names.

```
S1#show vlan brief

VLAN Name                         Status    Ports
---- ---------------------------- --------- -------------------------------
1    default                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                            Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                            Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                            Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                            Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                            Gig1/1, Gig1/2
10   Faculty/Staff                active
20   Students                     active
30   Guest(Default)               active
```



```
99   Management&Native         active
1002 fddi-default              active
1003 token-ring-default        active
1004 fddinet-default           active
1005 trnet-default             active
```

If you enter the same command on S2 and S3, you will notice that the VLANs are not in their VLAN database? Why not?

_____

_____

Step 4. Check results.

Your completion percentage should be 46%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure Trunks on S1, S2, and S3

Use the **switchport mode trunk** command to set trunk mode for each of the trunk links. Use the **switchport trunk native vlan 99** command to set VLAN 99 as the native VLAN.

Step 1. Configure FastEthernet 0/1 and FastEthernet 0/3 on S1 for trunking.

Enter the appropriate commands to configure trunking and set VLAN 99 as the native VLAN.

Once configured, Dynamic Trunking Protocol (DTP) will bring up the trunk links. You can verify S2 and S3 are now trunking by entering the **show interface fa0/1 switchport** command on S2 and the **show interface fa0/3 switchport** command on S3.

If you wait a few minutes for Packet Tracer to simulate all the processes, S1 will advertise the VLAN configuration to S2 and S3. This can be verified on S2 or S3 with both the **show vlan brief** command and the **show vtp status** command.

However, it is a best practice to configure both sides of the trunk links to the **on** mode.

Step 2. Configure Fast Ethernet 0/1 on S2 for trunking.

Enter the appropriate commands to configure trunking and set VLAN 99 as the native VLAN.

Step 3. Configure Fast Ethernet 0/3 on S3 for trunking.

Enter the appropriate commands to configure trunking and set VLAN 99 as the native VLAN.

Step 5. Check results.

Your completion percentage should be 77%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Verify VTP Status

Using the **show vtp status** and **show vlan brief** commands, verify the following.

- S1 should show server status
- S2 and S3 should show client status
- S2 and S3 should have VLANs from S1

Note: VTP advertisements are flooded throughout the management domain every five minutes or whenever a change occurs in VLAN configurations. To accelerate this process, you can switch between

Realtime mode and Simulation mode until the next round of updates. However, you may have to do this multiple times since this will only forward Packet Tracer's clock by 10 seconds each time. Alternatively, you can change one of the client switches to transparent mode and then back to client mode.

What is the configuration revision number? _____

Why is the configuration revision number higher than the number of VLANs you created?

_____

_____

What is the current number of existing VLANs? _____

Why are there more existing VLANs than the four you created?

_____

Completion should still be at 77% at the end of this Task.

Task 7: Assign VLANs to Ports

Use the **switchport mode access** command to set access mode for the access links. Use the **switchport access vlan** *vlan-id* command to assign a VLAN to an access port.

Step 1. Assign VLANs to ports on S2.

- Fa0/11 on VLAN 10
- Fa0/18 on VLAN 20
- Fa0/6 on VLAN 30

Step 2. Assign VLANs to ports on S3.

- Fa0/11 on VLAN 10
- Fa0/18 on VLAN 20
- Fa0/6 on VLAN 30

Step 4. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Verify VLAN Implementation and Test Connectivity

Step 1. Verify VLAN configuration and port assignments.

Use the **show vlan brief** command to verify VLAN configuration and port assignments on each switch. Compare your output to the topology.

Step 2. Test connectivity between PCs.

Pings between PCs on the same VLAN should succeed, while pings between PCs on different VLANs should fail.

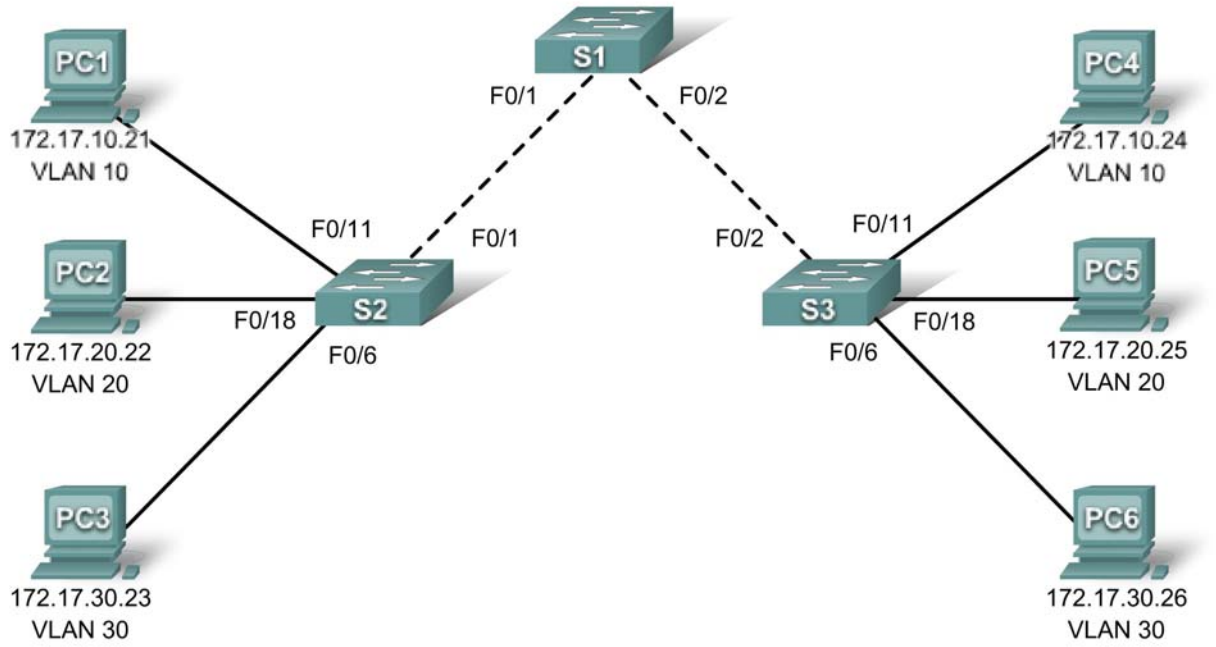
From PC1 ping PC4.

From PC2 ping PC5.

From PC3 ping PC6.

PT Activity 4.4.1: Basic VTP Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.11	255.255.255.0	N/A
S2	**VLAN 99**	172.17.99.12	255.255.255.0	N/A
S3	**VLAN 99**	172.17.99.13	255.255.255.0	N/A
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**NIC**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**NIC**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**NIC**	172.17.30.26	255.255.255.0	172.17.30.1

Port Assignments (S2 and S3)

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 - 0/10	VLAN 30 - Guest (Default)	172.17.30.0 /24
Fa0/11 - 0/17	VLAN 10 - Faculty/Staff	172.17.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Students	172.17.20.0 /24

Learning Objectives

- Perform basic switch configurations
- Configure the Ethernet interfaces on the host PCs
- Configure VTP and security on the switches

Introduction

In this activity, you will perform basic switch configurations, configure VTP, trunking, learn about VTP modes, create and distribute VLAN information and assign ports to VLANs. The initial network opens in a secure state with all ports administratively shutdown.

Task 1: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

- Configure the switch hostname as indicated on the topology.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```


Task 2: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, PC5, and PC6 with the IP addresses and default gateways indicated in the addressing table.

Task 3: Configure VTP and Security on the Switches

Step 1. Enable the user ports on S2 and S3.

Configure the user ports in access mode. Refer to the topology diagram to determine which ports are connected to end-user devices.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

Step 2. Check the current VTP settings on the three switches.

Use the show vtp status command to determine the VTP operating mode for all three switches.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
```



```
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

VTP allows the network administrator to control the instances of VLANs on the network by creating VTP domains. Within each VTP domain, one or more switches are configured as VTP servers. VLANs are then created on the VTP server and pushed to the other switches in the domain. Common VTP configuration tasks are setting the operating mode, domain, and password. Note that all three switches are in server mode. Server mode is the default VTP mode for most Catalyst switches. In this activity, you will be using S1 as the VTP server, with S2 and S3 configured as VTP clients or in VTP transparent mode.

Step 3. Configure the operating mode, domain name, and VTP password on all three switches.

Set the VTP domain name to Lab4 and the VTP password to cisco on all three switches. Configure S1 in server mode, S2 in client mode, and S3 in transparent mode.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end

S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end

S3(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
S3(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Note: The VTP domain name can be learned by a client switch from a server switch, but only if the client switch domain is in the null state. It does not learn a new name if one has been previously set. For that reason, it is good practice to manually configure the domain name on all switches to ensure that the domain name is configured correctly. Switches in different VTP domains do not exchange VLAN information.

Step 4. Configure trunking and the native VLAN for the trunking ports on all three switches.

On all switches, configure trunking and the native VLAN for FastEthernet interfaces 0/1-5. Only commands for fa0/1 on each switch are shown below.

```
S1(config)#interface fa0/1
```



```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config-if)#interface fa0/2
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config-if)#end

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#no shutdown
S2(config-if)#end

S3(config)#interface fa0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#no shutdown
S3(config-if)#end
```

Step 5. Configure port security on the S2 and S3 access layer switches.

Configure ports fa0/6, fa0/11, and fa0/18 so that they allow only a single host and learn the MAC address of the host dynamically.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end

S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Step 6. Configure VLANs on the VTP server.

There are four VLANS required in this lab:

- VLAN 99 (management)

- VLAN 10 (faculty/staff)
- VLAN 20 (students)
- VLAN 30 (guest)

Configure these on the VTP server. Packet Tracer grading is case-sensitive.

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit
```

Verify that the VLANs have been created on S1 with the show vlan brief command.

Step 7. Check if the VLANs created on S1 have been distributed to S2 and S3.

Use the show vlan brief command on S2 and S3 to determine if the VTP server has pushed its VLAN configuration to all the switches.

```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
10   faculty/staff                     active
20   students                          active
30   guest                             active
99   management                        active

S3#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                 Gig1/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Are the same VLANs configured on all switches? _____Why do S2 and S3 have different VLAN configurations at this point?

Step 8. Create a new VLAN on S2 and S3.

```
S2(config)#vlan 88
%VTP VLAN configuration not allowed when device is in CLIENT mode.

S3(config)#vlan 88
S3(config-vlan)#name test
S3(config-vlan)#
```

Why are you prevented from creating a new VLAN on S2 but not S3?

Delete VLAN 88 from S3.

```
S3(config)#no vlan 88
```

Step 9. Manually configure VLANs.

Configure the four VLANs identified in Step 6 on switch S3.

```
S3(config)#vlan 99
S3(config-vlan)#name management
S3(config-vlan)#exit
S3(config)#vlan 10
S3(config-vlan)#name faculty/staff
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name students
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name guest
S3(config-vlan)#exit
```

Here you see one of the advantages of VTP. Manual configuration is tedious and error prone, and any error introduced here could prevent intra-VLAN communication. In addition, these types of errors can be difficult to troubleshoot.

Step 10. Configure the management interface address on all three switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? If not, troubleshoot the switch configurations and try again.

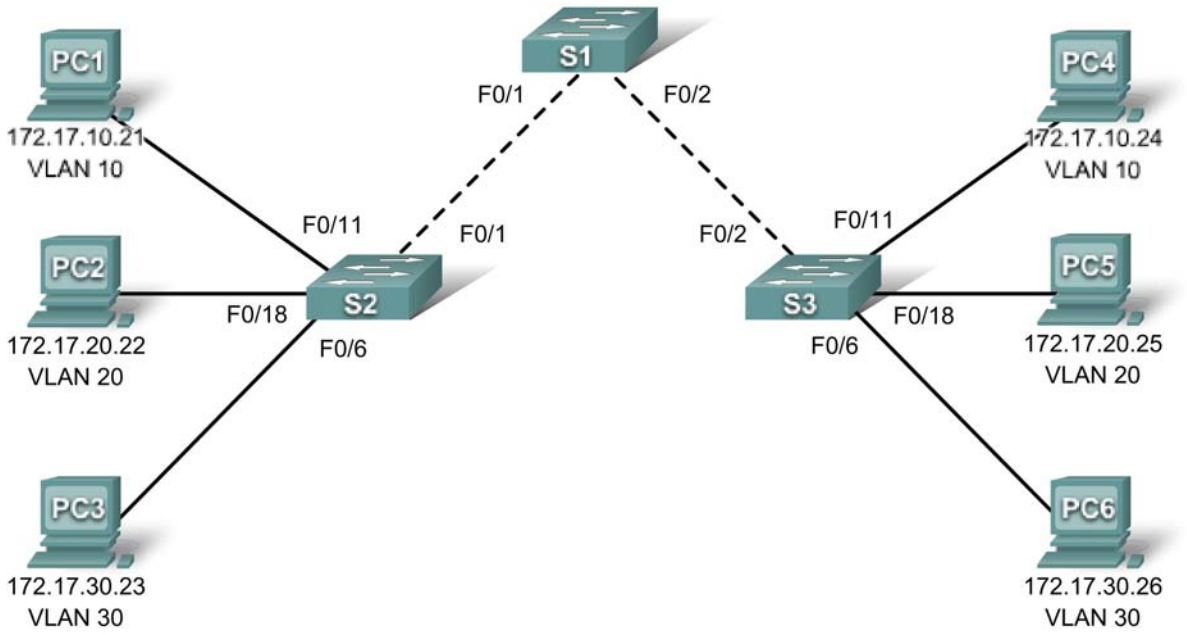
Step 11. Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the activity to assign ports to the VLANs. Since Packet Tracer 4.11 does not make use of the interface range command, only configure the first interface for each VLAN. Port assignments are not configured through VTP. Port assignments must be configured on each switch manually or dynamically using a VMPS server. The commands are shown for S3 only, but both S2 and S3 switches should be similarly configured. Save the configuration when you are done.

```
S3(config)#interface fa0/6
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface fa0/11
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface fa0/18
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S3#
```


PT Activity 4.4.2: VTP Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	**VLAN 99**	172.31.99.11	255.255.255.0
S2	**VLAN 99**	172.31.99.12	255.255.255.0
S3	**VLAN 99**	172.31.99.13	255.255.255.0
PC1	**NIC**	172.31.10.1	255.255.255.0
PC2	**NIC**	172.31.20.1	255.255.255.0
PC3	**NIC**	172.31.30.1	255.255.255.0
PC4	**NIC**	172.31.10.2	255.255.255.0
PC5	**NIC**	172.31.20.2	255.255.255.0
PC6	**NIC**	172.31.30.2	255.255.255.0

Port Assignments (S2 and S3)

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks	
Fa0/6 - 0/10	VLAN 30 - Administration	172.31.30.0 /24
Fa0/11 - 0/17	VLAN 10 - Engineering	172.31.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Sales	172.31.20.0 /24
None	VLAN 99 – Network Mgmt	172.31.99.0 /24

Learning Objectives

- Perform basic switch configurations
- Configure the Ethernet interfaces on the host PCs
- Configure VTP the switches

Introduction

In this activity, you will perform basic switch configurations, configure VTP, trunking, learn about VTP modes, create and distribute VLAN information and assign ports to VLANs

Task 1: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

- Configure the switch hostname as indicated on the topology.
- Disable DNS lookup.
- Configure an EXEC mode password of class.
- Configure a password of cisco for console and vty connections.

Task 2: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, PC5, and PC6 with the IP addresses indicated in the addressing table. Default gateway configurations are not necessary for this activity.

Task 3: Configure VTP on the Switches

VTP allows the network administrator to control the instances of VLANs on the network by creating VTP domains. Within each VTP domain, one or more switches are configured as VTP servers. VLANs are then created on the VTP server and pushed to the other switches in the domain. Common VTP configuration tasks are operating mode, domain, and password. In this lab, you will be configuring S1 as a VTP server, with S2 and S3 configured as VTP clients.

Step 1. Check the current VTP settings on the three switches.

Step 2. Configure the operating mode, domain name, and VTP password on all three switches.

Set the VTP domain name to **access** and the VTP password to **lab4** on all three switches. Configure S1 in server mode, S2 in client mode, and S3 in transparent mode. Packet Tracer will initially grade the mode for S3 as incorrect. You will correct it later in the activity.

Note: The VTP domain name can be learned by a client switch from a server switch, but only if the client switch domain is in the null state. It does not learn a new name if one has been previously set. For that reason, it is good practice to manually configure the domain name on all switches to ensure that the domain name is configured correctly. Switches in different VTP domains do not exchange VLAN information.

Step 3. Configure trunking and the native VLAN for the trunking ports on all three switches.

On all switches, configure trunking and the native VLAN for FastEthernet interfaces 0/1-5.

Step 4. Configure port security on the S2 and S3 access layer switches.

Configure ports Fa0/6, Fa0/11, and Fa0/18 on S2 and S3 so that they allow a maximum of two hosts to connect to these ports and learn the MAC addresses of the hosts dynamically.

Step 5. Configure VLANs on the VTP server.

There are four VLANS required in this lab:

- VLAN 99 management
- VLAN 10 engineering
- VLAN 20 sales
- VLAN 30 administration

Configure these on the VTP server.

When you are done, verify that all four VLANs have been created on S1.

Step 6. Check if the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to determine if the VTP server has pushed its VLAN configuration to all the switches.

Are the same VLANs configured on all switches? _____

Why do S2 and S3 have different VLAN configurations at this point? _____

_____

_____

Step 7. Configure the management interface address on all three switches.

Before proceeding, change the VTP mode on S3 to client. Then verify that S3 received VLAN configurations from S1 through VTP.

Configure all three switches with the IP addresses identified in the addressing table at the beginning of the lab. Assign these addresses to the network management VLAN (VLAN 99).

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? _____

If not, troubleshoot the switch configurations and resolve.

Step 8. Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the lab to assign ports to VLANs. Note that port assignments are not configured through VTP. Remember that both S2 and S3 switches should be similarly configured. Save the configuration when you are done.

Step 9. Verify that the trunks are operating correctly.

From PC1, attempt to ping PC4, PC5, and PC6.

Were any of the pings successful? _____

Why did some of the pings fail?

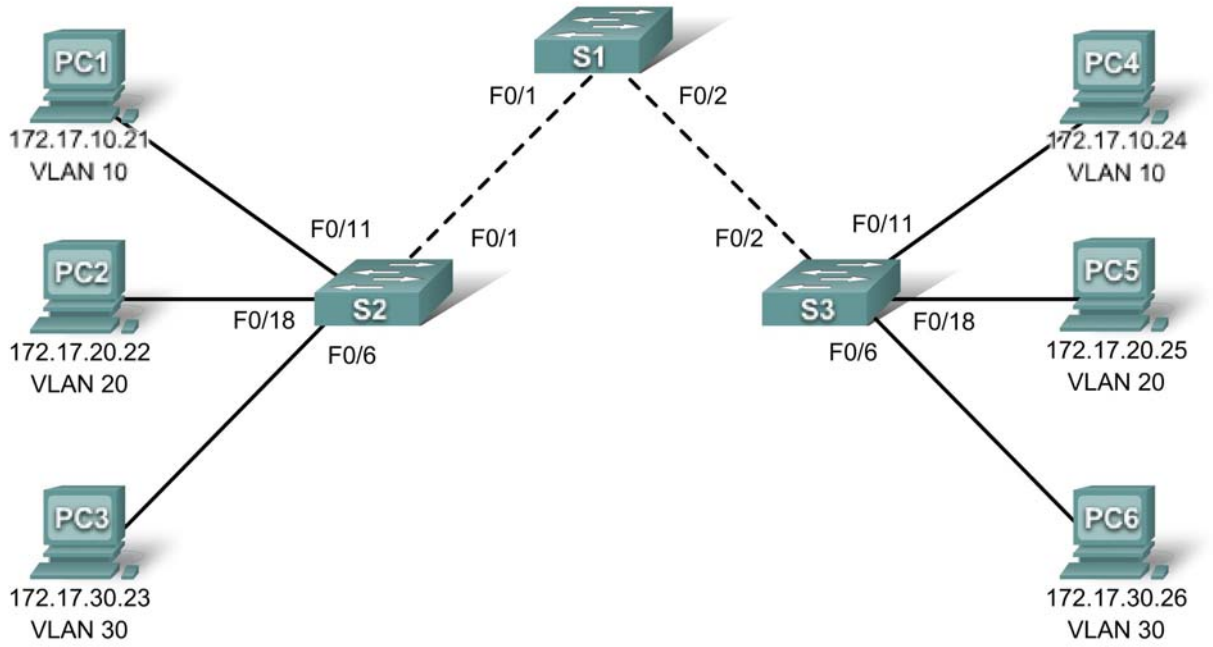
_____

_____

Which hosts could be reached from PC3? _____

PT Activity 4.4.3: Troubleshooting the VTP Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	**VLAN 99**	172.17.99.11	255.255.255.0
S2	**VLAN 99**	172.17.99.12	255.255.255.0
S3	**VLAN 99**	172.17.99.13	255.255.255.0
PC1	**NIC**	172.17.10.21	255.255.255.0
PC2	**NIC**	172.17.20.22	255.255.255.0
PC3	**NIC**	172.17.30.23	255.255.255.0
PC4	**NIC**	172.17.10.24	255.255.255.0
PC5	**NIC**	172.17.20.25	255.255.255.0
PC6	**NIC**	172.17.30.26	255.255.255.0

Port Assignments (S2 and S3)

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 - 0/10	VLAN 30 - Guest (Default)	172.17.30.0 /24
Fa0/11 - 0/17	VLAN 10 - Faculty/Staff	172.17.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Students	172.17.20.0 /24

Learning Objectives

- Find and correct all configuration errors
- Document the corrected network

Introduction

The VLAN Trunking Protocol (VTP) helps ensure uniform VLAN configurations on your switched network, but it must be configured correctly. In this activity, the VTP domain name is **Lab3_4**, and the VTP password is **cisco**. However, there are a number of errors in this configuration that you must troubleshoot and correct before end-to-end connectivity within the VLAN is restored. You will have successfully resolved all errors when the same VLANs are configured on all three switches, and you can ping between any two hosts in the same VLAN or between any two switches.

Task 1: Troubleshoot and Correct VTP and Configuration Errors

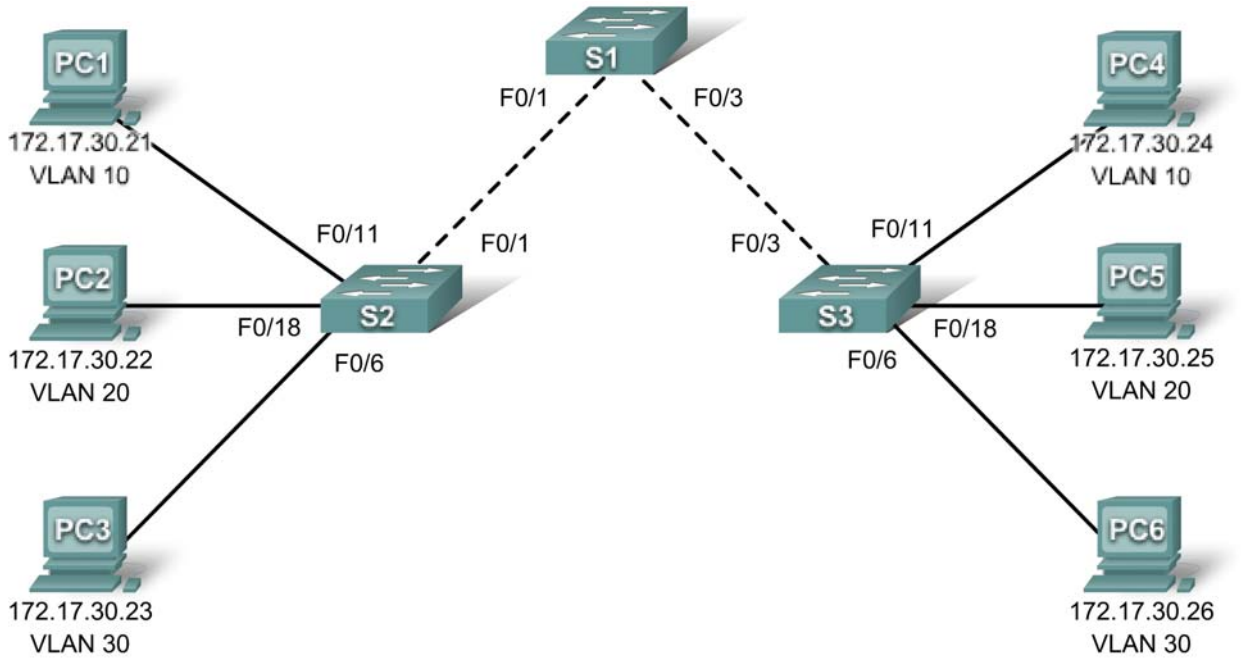
When all errors are corrected, you should be able to ping PC4 from PC1, PC5 from PC2, and PC6 from PC3. You should also be able to ping the management interfaces on both S2 and S3 from S1.

Task 2: Document the Switch Configuration

When you have completed your troubleshooting, capture the output of the **show run** command and save it to a text document for each switch.

PT Activity 4.5.1: Packet Tracer Skills Integration Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.31	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.32	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.33	255.255.255.0	172.17.99.1
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**NIC**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**NIC**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**NIC**	172.17.30.26	255.255.255.0	172.17.30.1

Learning Objectives:

- Configure and verify basic device configurations
- Configure and verify port security
- Configure VTP
- Configure trunking

- Configure VLANs
- Assign VLANs to ports
- Verify end-to-end connectivity

Introduction

In this activity, you will configure switches including basic configuration, port security, trunking and VLANs. You will use VTP to advertise the VLAN configurations to other switches.

Task 1: Configure and Verify Basic Device Configurations

Step 1. Configure basic commands.

Configure each switch with the following basic commands. Packet Tracer will only grade the **hostname** command.

- Hostname on S1
- Banner
- Enable secret password
- Line configurations
- Service encryption

Step 2. Configure the management VLAN interface on S1, S2, and S3.

Create and enable interface VLAN 99 on each switch. Use the addressing table for address configuration.

Step 3. Verify PCs on the same subnet can ping each other.

The PCs are already configured with correct addressing. Create Simple PDUs to test connectivity between devices on the same subnet:

Step 4. Check results.

Your completion percentage should be 15%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure and Verify Port Security

Step 1. Configure all access links with port security.

Normally you configure port security on all access ports or shutdown the port if it is not in use. Use the following policy to establish port security just on the ports used by the PCs.

- Set the port to access mode.
- Enable port security.
- Allow only 1 MAC address.
- Configure the first learned MAC address to "stick" to the configuration.
- Set the port to shutdown if there is a security violation.
- Force the switches to learn the MAC addresses by sending pings across all three switches.

NOTE: Only enabling port security is graded by Packet Tracer. However, all the port security tasks listed above are required to complete this activity.

Step 2. Test port security.

- Connect PC2 to PC3's port and connect PC3 to PC2's port.
- Send pings between PCs on the same subnet.
- The ports for PC2 and PC3 should shutdown.

Step 3. Verify ports are "err-disabled" and that a security violation has been logged.

Step 4. Reconnect PCs to correct port and clear port security violations.

- Connect PC2 and PC3 back to the correct port.
- Clear the port security violation.
- Verify PC2 and PC3 can now send pings across S2.

Step 5. Check results.

Your completion percentage should be 55%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure VTP

Step 1. Configure the VTP mode on all three switches.

Configure S1 as the server. Configure S2 and S3 as clients.

Step 2. Configure the VTP domain name on all three switches.

Use **CCNA** as the VTP domain name.

Step 3. Configure VTP domain password on all three switches.

Use **cisco** as the VTP domain password.

Step 4. Check results.

Your completion percentage should be 70%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure Trunking

Step 1. Configure trunking on S1, S2, and S3.

Configure the appropriate interfaces in trunking mode and assign VLAN 99 as the native VLAN.

Step 2. Check results.

Your completion percentage should be 83%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure VLANs

Step 1. Create the VLANs on S1.

Create and name the following VLANs on S1 only. VTP will advertise the new VLANs to S1 and S2.

- VLAN 10 **Faculty/Staff**
- VLAN 20 **Students**

- VLAN 30 **Guest(Default)**
- VLAN 99 **Management&Native**

Step 2. Verify VLANs have been sent to S2 and S3.

Use appropriate commands to verify that S2 and S3 now have the VLANs you created on S1. It may take a few minutes for Packet Tracer to simulate the VTP advertisements.

Step 3. Check results.

Your completion percentage should be 90%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Assign VLANs to ports

Step 1. Assign VLANs to access ports on S2 and S3.

Assign the PC access ports to VLANs:

- VLAN 10: PC1 and PC4
- VLAN 20: PC2 and PC5
- VLAN 30: PC3 and PC6

Step 2. Verify VLAN implementation.

Use the appropriate command to verify your VLAN implementation.

Step 3. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Verify End-to-End Connectivity

Step 1. Verify PC1 and PC4 can ping each other.

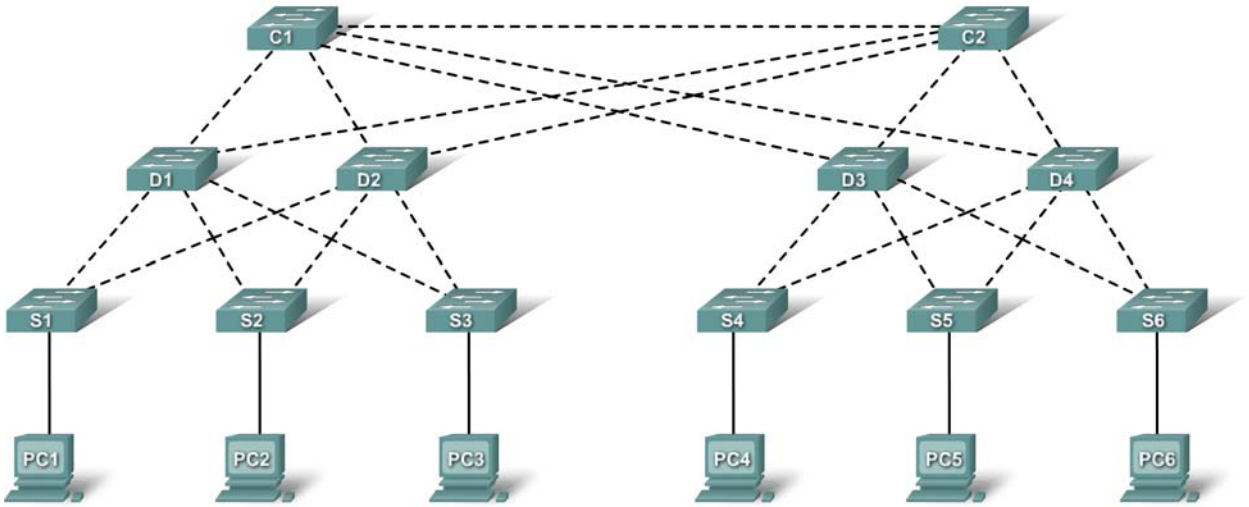
Step 2. Verify PC2 and PC5 can ping each other.

Step 3. Verify PC3 and PC6 can ping each other.

Step 4. PCs on different VLANs should not be able to ping each other.

PT Activity 5.1.3: Examining a Redundant Design

Topology Diagram



Learning Objectives

- Check for STP convergence
- Examine the ARP process
- Test redundancy in a switched network

Introduction

In this activity, you will examine how STP operates by default. Switches have been added to the network "out of the box." Cisco switches can be plugged in and connected to a network without any additional action by the network administrator. Therefore these switches will act according to default settings.

Task 1: Check for STP Convergence

When STP is fully converged, the following conditions exist:

- All PCs have green link lights on the switched ports.
- Access layer switches have one forwarding uplink (green) to a distribution layer switch and a blocking uplink (amber) to a second distribution layer switch.
- Distribution layer switches have one forwarding uplink (green) to a core layer switch and a blocking uplink (amber) to another core layer switch.

Task 2: Examine the ARP Process

Step 1. Switch to Simulation mode.

Step 2. Ping from PC1 to PC6.

Use the Add Simple PDU tool to create a PDU from PC1 to PC6. Be sure ICMP is selected in the **Event List Filters**. Click **Capture/Forward** to examine the ARP process as the switched network learns the

MAC addresses of PC1 and PC6. Notice that all possible loops are stopped by blocking ports. For example, the ARP request from PC1 travels from S1 to D2 to C1 to D1 and then back to S1. However, because STP is blocking the link between S1 and D1, no loop occurs.

Notice that the ARP reply from PC6 travels back along one path. Why?

_____

_____

_____

Record the loop-free path between PC1 and PC6.

_____

_____

Step 3. Examine the ARP process again.

Examine the ARP process again by pinging between two different PCs.

What part of the path changed from the last set of pings?

_____

_____

Task 3: Test Redundancy in a Switched Network

Step 1. Delete the link between S1 and D2.

Switch to Realtime mode. Delete the link between S1 and D2. It takes some time for STP to converge and establish a new, loop-free path. Because only S1 is affected, watch for the amber light on the link between S1 and D1 to change to green.

Step 2. Ping between PC1 and PC6.

After the link between S1 and D1 is active (indicated by a green light), switch to Simulation mode and ping between PC1 and PC6 again.

Record the new loop-free path.

_____

_____

Step 3. Delete link between C1 and D3.

Switch to Realtime mode. Notice that the links between D3 and D4 to C2 are amber. Delete the link between C1 and D3. It will take some time for STP to converge and establish a new, loop-free path. Watch the amber links on D3 and D4. You can switch between Simulation mode and Realtime mode to accelerate the process.

Which link is now the active link to C2?

_____

_____

Step 4. Ping between PC1 and PC6.

Switch to Simulation mode and ping between PC1 and PC6.

Record the new loop-free path.

_____

_____

Step 5. Delete D4.

Switch to Realtime mode. Notice that S4, S5, and S6 are all forwarding traffic to D4. Delete D4. It takes some time for STP to converge and establish a new, loop-free path. Watch for the links between S4, S5, and S6 to D3 transition to forwarding (green). All three switches should now be forwarding to D3.

Step 6. Ping between PC1 and PC6.

Switch to Simulation mode and ping between PC1 and PC6.

Record the new loop-free path.

_____

_____

What is unique about the new path that you have not seen before?

_____

_____

_____

Step 7. Delete C1.

Switch to Realtime mode. Notice that D1 and D2 are both forwarding traffic to C1. Delete C1. It takes some time for STP to converge and establish a new, loop-free path. Watch for the links between D1 and D2 to C2 to transition to forwarding (green). Once converged, both switches should now be forwarding to C2.

Step 8. Ping between PC1 and PC6.

Switch to Simulation mode and ping between PC1 and PC6.

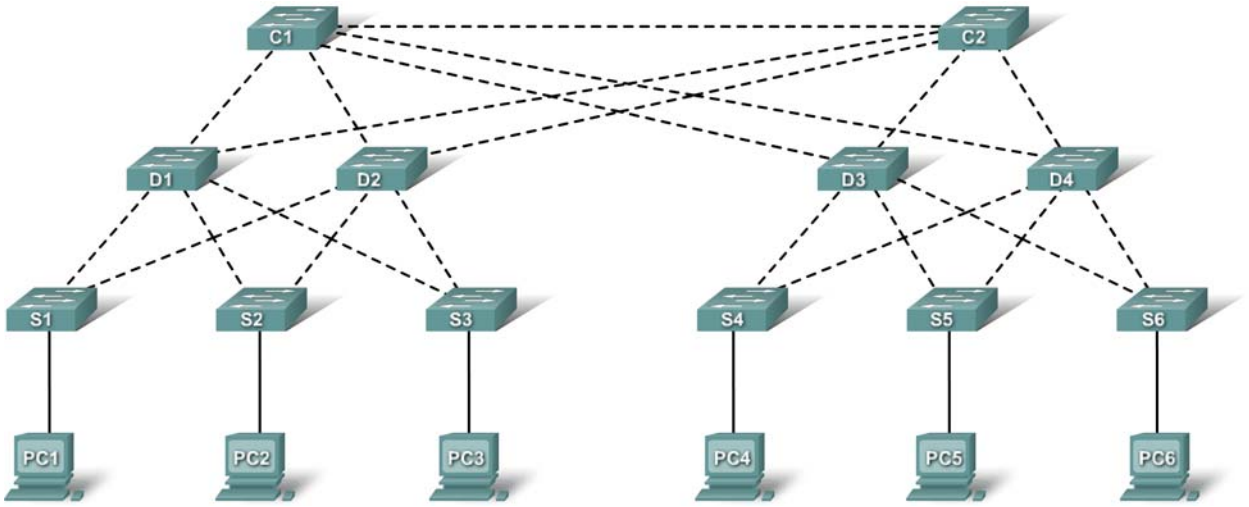
Record the new loop-free path.

_____

_____

PT Activity 5.2.5: Configuring STP

Topology Diagram



Learning Objectives

- Examine the STP default state
- Configure the root bridge
- Configure the backup root bridge
- Finalize STP configuration

Introduction

In this activity, the switches are “out of the box” without any configuration. You will manipulate the root bridge election so that the core switches are chosen before the distribution or access layer switches.

Task 1: Examine the STP Default State

Step 1. Examine link lights.

When STP is fully converged, the following conditions exist:

- All PCs have green link lights on the switched ports.
- Access layer switches have one forwarding uplink (green) to a distribution layer switch and a blocking uplink (amber) to a core layer switch.
- Distribution layer switches have one forwarding uplink (green) to a core layer switch and a blocking uplink (amber) to another core layer switch.

Step 2. Switch to Simulation mode.

Step 3. Determine the root bridge.

Click **Capture/Forward**. Without looking at BPDU detail, MAC addresses, or the **show spanning-tree** command, can you tell which switch is the root bridge?

_____

_____

Can you think of a reason why this switch is not a good choice as root?

_____

_____

Task 2: Configure the Root Bridge

Step 1. Configure the root bridge.

One of the core switches should be root, and the other should be the backup root. Switch to Realtime mode and configure C1 with a priority of **4096**.

Step 2. Switch between Realtime and Simulation modes.

Switch between Realtime mode and Simulation mode several times until all ports on C1 are green.

Step 3. Switch to Simulation mode.

Step 4. Make sure C1 is the root bridge.

Click **Capture/Forward** several times to watch configuration BPDUs. C1 should be initiating the propagation of BPDUs.

Step 5. Check results.

Your completion percentage should be 17%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure the Backup Root Bridge

Step 1. Configure the backup root bridge.

The other core switch serves as a backup root bridge. Switch to Realtime mode and configure C2 with a priority of **8192**.

Step 2. Switch between Realtime and Simulation modes.

Switch between Realtime mode and Simulation mode several times until all ports on C2 are green.

Step 3. Examine links attached to C2.

What is unique about the C2 links to the distribution layer switches that you do not see with C1 links?

_____

_____

Step 4. Check results.

Your completion percentage should be 33%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Finalize STP Configuration

Best practice is to never have an access layer switch become root. You could ensure this by configuring all access layer switches with a priority higher than the default. However, because there are fewer

distribution switches, it is more efficient to configure these switches with a slightly higher priority than the backup root switch.

Step 1. Configure distribution switches.

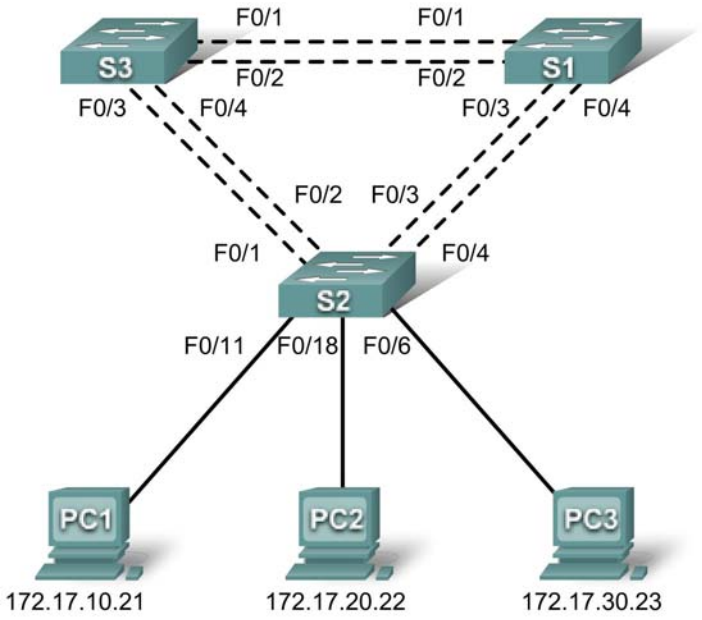
Configure D1, D2, D3, and D4 with a priority of **12288**.

Step 2. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 5.5.2: Challenge Spanning Tree Protocol

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.11	255.255.255.0	N/A
S2	**VLAN 99**	172.17.99.12	255.255.255.0	N/A
S3	**VLAN 99**	172.17.99.13	255.255.255.0	N/A
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.12
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.12
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.12

Port Assignments – S2

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 - 0/10	VLAN 30 – Guest(Default)	172.17.30.0 /24
Fa0/11 - 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Students	172.17.20.0 /24

Learning Objectives

- Perform basic switch configurations
- Configure the Ethernet interfaces on the host PCs
- Configure VLANs
- Configure spanning tree
- Optimizing STP

Introduction

In this activity, you will perform basic switch configurations, configure addressing on PCs, configure VLANs, examine the Spanning Tree Protocol and learn how to optimize it.

Task 1: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

Configure the switch hostname as indicated on the topology.

- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Task 2: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP address, subnet mask, and gateway indicated in the addressing table.

Task 3: Configure VLANs

Step 1. Enable the user ports on S2 in access mode.

Refer to the topology diagram to determine which switch ports on S2 are activated for end-user device access. These three ports will be configured for access mode and enabled with the no shutdown command.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

Step 2. Configure VTP.

Configure VTP on the three switches using the following table. Remember that VTP domain names and passwords are case-sensitive. The default operating mode is server.

Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Server	Lab5	cisco
S2	Client	Lab5	cisco
S3	Client	Lab5	cisco

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end

S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end

S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```


Step 3. Configure Trunk Links and Native VLAN.

Configure trunking ports and native VLAN. For each switch, configure ports Fa0/1 through Fa0/5 as trunking ports. Designate VLAN 99 as the native VLAN for these trunks. When this activity was started, these ports were disabled and must be re-enabled now using the **no shutdown** command.

Only the commands for the FastEthernet0/1 interface on each switch are shown, but the commands should be applied up to the FastEthernet0/5 interface.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config)#end

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#no shutdown
S2(config-if)#end

S3(config)#interface fa0/1
S3(config-if#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#no shutdown
S3(config-if-#end
```

Step 4. Configure the VTP server with VLANs.

VTP allows you to configure VLANs on the VTP server and have those VLANs populated to the VTP clients in the domain. This ensures consistency in the VLAN configuration across the network.

Configure the following VLANS on the VTP server:

VLAN	VLAN Name
VLAN 99	management
VLAN 10	faculty-staff
VLAN 20	students
VLAN 30	guest

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config)#vlan 10
S1(config-vlan)#name faculty-staff
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#end
```

Step 5. Verify the VLANs.

Use the **show vlan brief** command on S2 and S3 to verify that all four VLANs have been distributed to the client switches.

```
S2#show vlan brief
```



```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
10   faculty/staff                     active
20   students                          active
30   guest                             active
99   management                        active

S3#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 6. Configure the management interface address on all three switches.

```
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0

S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0

S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? If not, troubleshoot the switch configurations and try again.

Step 7. Assign switch ports to the VLANs.

Port assignments are listed in the table at the beginning of the activity. However, since Packet Tracer 4.11 does not support the **interface range** command, only assign the first port from each range.

```
S2(config)#interface fa0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fa0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fa0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
```



```
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S2#
```

Task 4: Configure Spanning Tree

Step 1. Examine the default configuration of 802.1D Spanning Tree Protocol (STP).

On each switch, display the spanning tree table with the **show spanning-tree** command. The output is shown for S1 only. Root selection varies depending on the default BID of each switch. In this activity S3 is currently the root.

```
S1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0050.0F68.146E
             Aging Time 300
```



```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr


VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    32798
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr


VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32768 sys-id-ext 99)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
```

Note that there are five instances of STP on each switch.

Examine the VLAN 99 spanning tree for all three switches:

```
S1#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32966 sys-id-ext 99)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
```



```
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr

S2#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32966 sys-id-ext 99)
             Address     00E0.F7AE.7258
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Altn BLK 19        128.3    Shr
Fa0/4            Altn BLK 19        128.3    Shr

S3#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0030.F20D.D6B1
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32966 sys-id-ext 99)
             Address     0030.F20D.D6B1
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
```

Step 2. Examine the output.

Answer the following questions based on the output.

What is the priority for switches S1, S2, and S3 on VLAN 99?

_____

What is the priority for S1 on VLANs 10, 20, 30, and 99?

_____

Which ports are blocking VLAN 99 on the root switch?

_____

Which ports are blocking VLAN 99 on the non-root switches?

_____

How does STP select the root?

_____

Since the bridge priorities are all the same, what else does the switch use to determine the root?

_____

Task 5: Optimizing STP

Because there is a separate instance of the spanning tree for every active VLAN, a separate root election is conducted for each instance. If the default switch priorities are used in root selection, the same root is elected for every spanning tree, as we have seen. This could lead to an inferior design. Some reasons to control the selection of the root switch include:

- The root switch is responsible for generating BPDUs in STP 802.1D and is the focal point for spanning tree control traffic. The root switch must be capable of handling this additional load.
- The placement of the root defines the active switched paths in the network. Random placement is likely to lead to suboptimal paths. Ideally the root is in the distribution layer.
- Consider the topology used in this activity. Of the six trunks configured, only two are carrying traffic. While this prevents loops, it is a waste of resources. Because the root can be defined on the basis of the VLAN, you can have some ports blocking for one VLAN and forwarding for another. This is demonstrated below.

In this example, it has been determined that the root selection using default values has led to under-utilization of the available switch trunks. Therefore, it is necessary to force another switch to become the root switch for VLAN 99 to impose some load-sharing on the trunks.

In the example output below, the default root switch for all VLANs is S3.

Selection of the root switch is accomplished by changing the spanning-tree priority for the VLAN. The default priority, as you have observed, is 32768 plus the VLAN ID. The lower number indicates a higher priority for root selection. Set the priority for VLAN 99 on S3 to 4096.

```
S1(config)#spanning-tree vlan 99 priority 4096
S1(config)#exit
```

Give the switches a little time to recalculate the spanning tree and then check the tree for VLAN 99 on switch S3 (the original VLAN 99 root) and switch S1 (the non-root switch selected to become the new VLAN 99 root).

```
S3#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    4195
             Address     0050.0F68.146E
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32867  (priority 32966 sys-id-ext 99)
             Address     0030.F20D.D6B1
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/1            Root FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
```



```
S1#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    4195
             Address     0050.0F68.146E
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4195  (priority 4294 sys-id-ext 99)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/1            Desg FWD 19        128.3    Shr
```

Which switch is the root for VLAN 99?

_____

Which ports are blocking VLAN 99 traffic on the new root?

_____

Which ports are now blocking VLAN 99 traffic on the old root?

_____

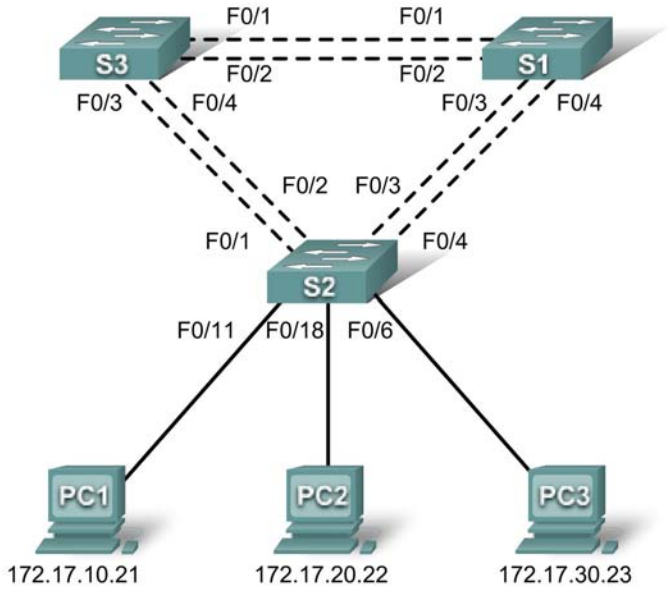
Compare the S1 VLAN 99 spanning tree above with the S1 VLAN 10 spanning tree.

```
S1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0030.F20D.D6B1
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32778  (priority 32788 sys-id-ext 10)
             Address     0050.0F68.146E
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/2            Altn BLK 19        128.3    Shr
Fa0/1            Root FWD 19        128.3    Shr
```

Note that S1 can now use all four ports for VLAN 99 traffic as long as they are not blocked at the other end of the trunk. However, the original spanning tree topology, with one of four S1 ports in blocking mode, is still in place for the four other active VLANs. By configuring groups of VLANs to use different trunks as their primary forwarding path, we retain the redundancy of failover trunks, without having to leaves trunks totally unused.

PT Activity 5.5.3: Troubleshooting Spanning Tree Protocol

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.11	255.255.255.0	N/A
S2	**VLAN 99**	172.17.99.12	255.255.255.0	N/A
S3	**VLAN 99**	172.17.99.13	255.255.255.0	N/A
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1

Port Assignments – S2

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 - 0/10	VLAN 30 – Guests(Default)	172.17.30.0 /24
Fa0/11 - 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Students	172.17.20.0 /24

Learning Objectives

- Identify the initial state of all trunks
- Correct the source of the problem
- Document the switch configuration

Scenario

You are responsible for the operation of the redundant switched LAN shown in the topology diagram. You and your users have been observing increased latency during peak usage times, and your analysis points to congested trunks. You recognize that of the six trunks configured, only two are forwarding packets in the default STP configuration currently running. The solution to this problem requires more effective use of the available trunks.

This activity is complete when all wired trunks are carrying traffic, and all three switches are participating in per-VLAN load balancing for the three user VLANs.

Task 1: Identify the Initial State of All Trunks

On each of the switches, display the spanning tree table with the **show spanning-tree** command. Note which ports are forwarding on each switch, and identify which trunks are not being used in the default configuration. You can use your network topology drawing to document the initial state of all trunk ports.

Task 2: Correct the Source of the Problem

Modify the spanning tree configuration so that all three trunks are in use. Assume that the three user LANs (10, 20, and 30) carry an equal amount of traffic. Aim for a solution that will have a different set of ports forwarding for each of the three user VLANs.

In order for the activity to be correctly graded, you must meet the following guidelines:

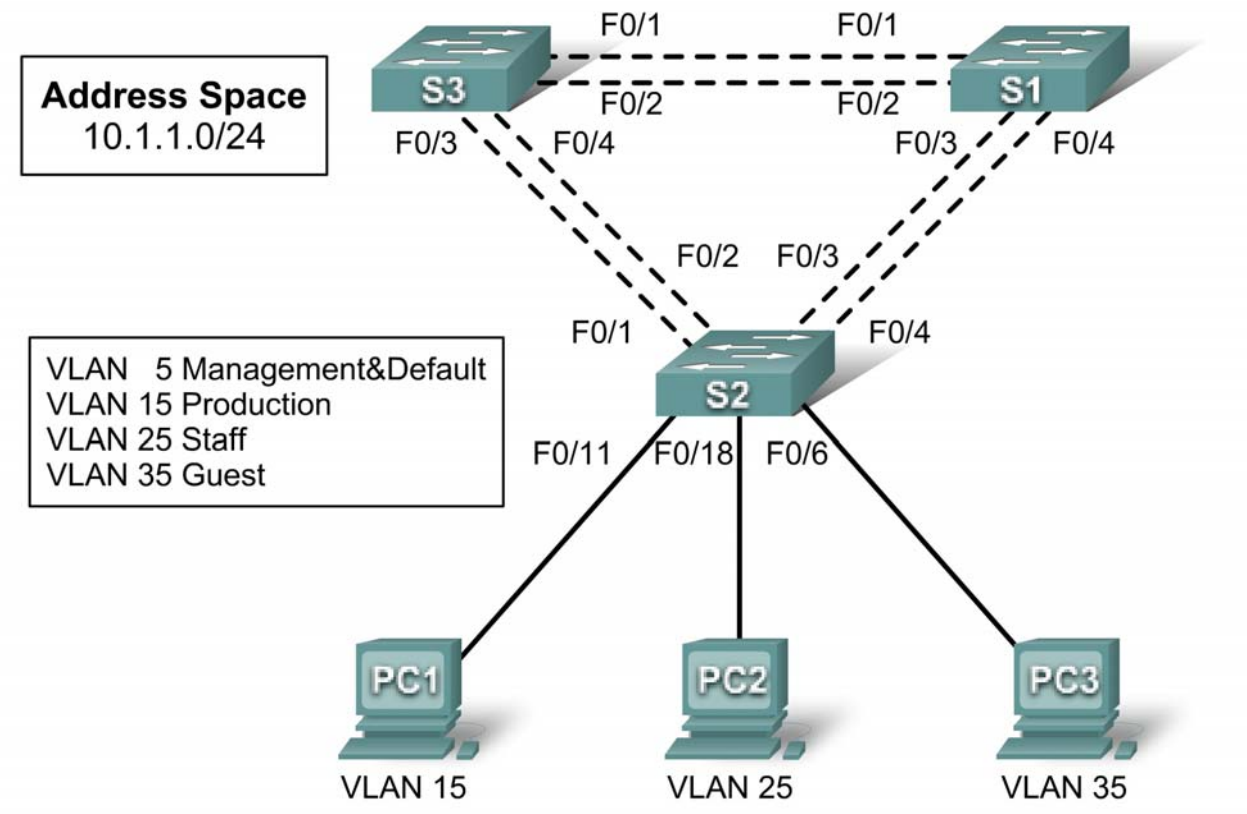
- S1 is root for VLAN 10 (priority 4096) and backup root for VLAN 20 (priority 16384)
- S2 is root for VLAN 20 (priority 4096) and backup root for VLAN 30 (priority 16384)
- S3 is root for VLAN 30 (priority 4096) and backup root for VLAN 10 (priority 16384)

Task 3: Document the Switch Configuration

When you have completed your solution, capture the output of the **show run** command and save it to a text file for each switch.

PT Activity 5.6.1: Packet Tracer Skills Integration Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 5			
S2	VLAN 5			
S3	VLAN 5			
PC1	NIC			
PC2	NIC			
PC3	NIC			

Learning Objectives

- Design and document an addressing scheme
- Configure and verify basic device configurations
- Configure VTP
- Configure trunking
- Configure VLANs
- Assign VLANs to ports
- Configure STP
- Configure host PCs

Introduction

In this activity, you will configure a redundant network with VTP, VLANs, and STP. In addition, you will design an addressing scheme based on user requirements. The VLANs in this activity are different than what you have seen in previous chapters. It is important for you to know that the management and default VLAN does not have to be 99. It can be any number you choose. Therefore, we use VLAN 5 in this activity.

Task 1: Design and Document an Addressing Scheme

Your addressing scheme needs to satisfy the following requirements:

- Production VLAN needs 100 host addresses
- Staff VLAN needs 50 host addresses
- Guest VLAN needs 20 host addresses
- Management&Native VLAN needs 10 host address

Task 2: Configure and Verify Basic Device Configurations

Step 1. Configure basic commands.

Configure each switch with the following basic commands. Packet Tracer only grades the hostnames and default gateways.

- Hostnames
- Banner
- Enable secret password
- Line configurations
- Service encryption
- Default gateways

Step 2. Configure the management VLAN interface on S1, S2, and S3.

Create and enable interface VLAN 5 on each switch. Use your addressing scheme for the address configuration.

Step 3. Check results.

Your completion percentage should be 18%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure VTP

Step 1. Configure the VTP mode on all three switches.

Configure S1 as the server. Configure S2 and S3 as clients.

Step 2. Configure the VTP domain name on all three switches.

Use **XYZCORP** as the VTP domain name.

Step 3. Configure the VTP domain password on all three switches.

Use **westbranch** as the VTP domain password.

Step 4. Check results.

Your completion percentage should be 30%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure Trunking

Step 1. Configure trunking on S1, S2, and S3.

Configure the appropriate interfaces in trunking mode and assign VLAN 5 as the native VLAN.

Step 2. Check results.

Your completion percentage should be 66%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure VLANs

Step 1. Create the VLANs on S1.

Create and name the following VLANs on S1 only. VTP will advertise the new VLANs to S1 and S2.

- VLAN 15 **Production**
- VLAN 25 **Staff**
- VLAN 35 **Guest(Default)**
- VLAN 5 **Management&Native**

Step 2. Verify that VLANs have been sent to S2 and S3.

Use appropriate commands to verify that S2 and S3 now have the VLANs you created on S1. It may take a few minutes for Packet Tracer to simulate the VTP advertisements.

Step 3. Check results.

Your completion percentage should be 72%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Assign VLANs to Ports

Step 1. Assign VLANs to access ports on S2.

Assign the PC access ports to VLANs:

- VLAN 15: PC1 connected to Fa0/11
- VLAN 25: PC2 connected to Fa0/18
- VLAN 35: PC3 connected to Fa0/6

Step 2. Verify VLAN implementation.

Use appropriate command to verify your VLAN implementation.

Step 3. Check results.

Your completion percentage should be 81%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure STP

Step 1. Ensure that S1 is the root bridge.

Set the priority level on S1 so that it is always the root bridge for all VLANs.

Step 2. Verify that S1 is the root bridge.

Step 3. Check results.

Your completion percentage should be 87%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Configure Host PCs

Step 1. Configure the host PCs.

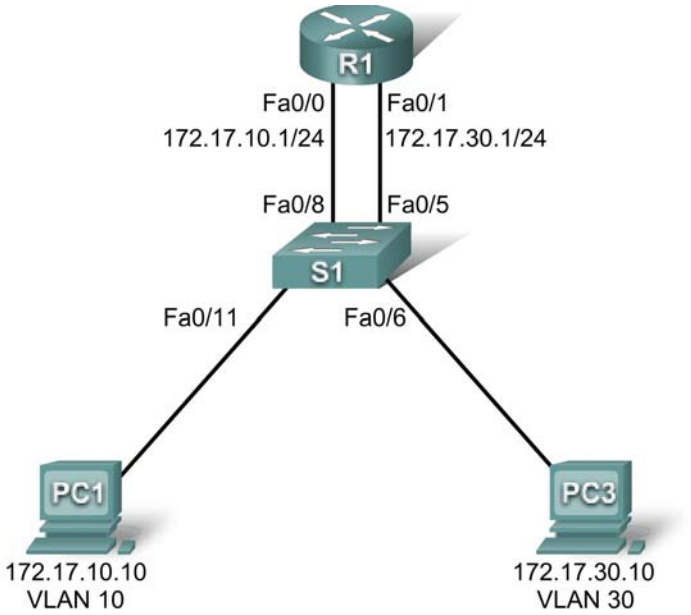
Use your addressing scheme to configure the PCs Fast Ethernet interface and default gateway.

Step 2. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 6.2.2.4: Configuring Traditional Inter-VLAN Routing

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	172.17.10.1	255.255.255.0	N/A
	Fa0/1	172.17.30.1	255.255.255.0	N/A
PC1	**NIC**	172.17.10.10	255.255.255.0	172.17.10.1
PC3	**NIC**	172.17.30.10	255.255.255.0	172.17.30.1

Learning Objectives

- Test connectivity without inter-VLAN routing
- Add VLANs to a switch
- Configure IP addressing on a router
- Test connectivity with inter-VLAN routing

Introduction

In this activity, you will configure traditional inter-VLAN routing simply by configuring two Fast Ethernet interfaces on a router. R1 has two connections to S1—one for each of the two VLANs. S1 and R1 already have basic configurations. The user EXEC password is **cisco,** and the privileged EXEC password is **class**. You will complete the configuration by adding VLANs to S1 and assigning VLANs to the correct ports. Then you will configure R1 with IP addressing. In traditional inter-VLAN routing, there are no additional, VLAN-related configurations needed on R1.

Task 1: Test Connectivity without Inter-VLAN Routing

Step 1. Ping between PC1 and PC3.

Wait for switch convergence. The link lights on the switch connecting to PC1 and PC3 change from amber to green. When the link lights are green, ping between PC1 and PC3. Because the two PCs are on separate networks and the router is not configured, they cannot communicate with one another, so the ping fails.

Step 2. Switch to simulation mode to monitor pings.

- Switch to simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.
- Click **Capture/Forward** to see the steps the ping takes between PC1 and PC3.
- Notice how the ping cannot even cross the switch.

Your completion percentage should be 0%.

Task 2: Add VLANs

Step 1. Create VLANs on S1.

Create two VLANs on S1, one for PC1 and one for PC3. PC1 belongs to VLAN 10, and PC3 belongs to VLAN 30. To create the VLANs, issue the **vlan 10** and **vlan 30** commands in global configuration mode.

```
S2#configure terminal
S2(config)#vlan 10
S2(config-vlan)#vlan 30
```

To check whether the VLANs were created, issue the **show vlan brief** command from the privileged EXEC prompt.

```
S2#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10   VLAN0010                          active
30   VLAN0030                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 2. Assign the VLANs to ports.

Each port on the switch is assigned to a VLAN to allow for inter-VLAN communication.

Assign the switch ports as follows:

- Assign the Fa0/5 and Fa0/6 interfaces to VLAN 30.
- Assign the Fa0/8 and Fa0/11 interfaces to VLAN 10.

To assign a VLAN to a port, enter the interface configuration. For Fa0/8, the command is **interface fa0/8**. The **switchport access vlan 10** assigns VLAN 10 to that port. The **switchport mode access** command sets the port to access mode.

```
S2(config)#interface fa0/8
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
```

Repeat the above steps for Fa0/5, Fa0/6, and Fa0/11, assigning the correct VLANs to each interface.

Step 3. Test connectivity between PC1 and PC3.

Now issue a ping between PC1 and PC3. The ping should still fail.

Step 4. Check results.

Your completion percentage should be 45%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure IP Addressing

Step 1. Configure IP addressing on R1.

Configure the Fa0/0 interface of R1 with the IP address 172.17.10.1 and subnet mask 255.255.255.0.

Configure the Fa0/1 interface with the IP address 172.17.30.1 and subnet mask 255.255.255.0.

Issue the **no shutdown** command on both interfaces to bring them up.

```
R1(config)#interface fa0/0
R1(config-if)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface fa0/1
R1(config-if)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#no shutdown
```

Step 2. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Test Connectivity Again

Step 1. Ping between PC1 and PC3.

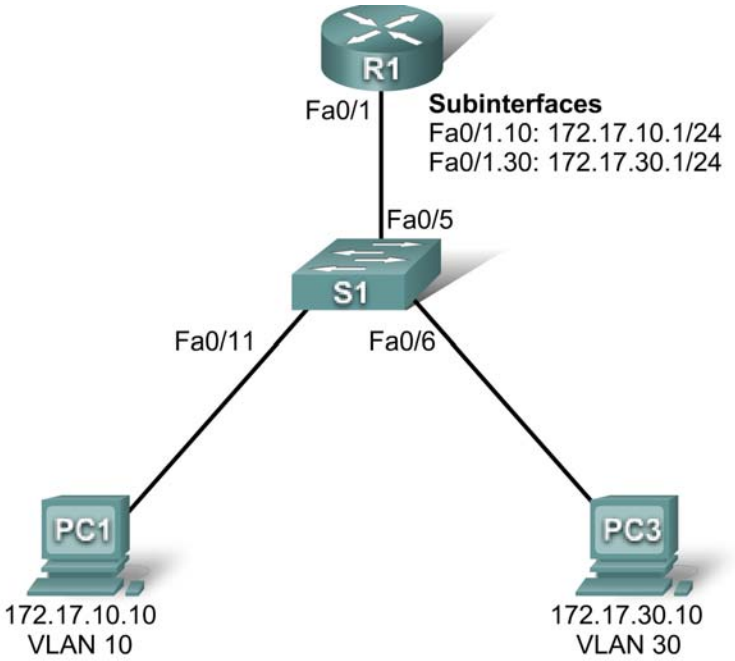
Wait for STP to converge. Then ping from PC1 to PC3. The ping should succeed.

Step 2. Switch to simulation mode to monitor pings.

- Switch to simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.
- Click **Capture/Forward** to see the steps the ping takes between PC1 and PC3.
- Watch as the ping goes from PC1 through S1, then to R1, then back to S1, and finally to the PC3.

PT Activity 6.2.2.5: Configuring Router-on-a-Stick Inter-VLAN Routing

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/1.10**	172.17.10.1	255.255.255.0	N/A
	Fa0/1.30	172.17.30.1	255.255.255.0	N/A
PC1	**NIC**	172.17.10.10	255.255.255.0	172.17.10.1
PC3	**NIC**	172.17.30.10	255.255.255.0	172.17.30.1

Learning Objectives

- Test connectivity without inter-VLAN routing
- Add VLANs to a switch
- Configure IP addressing on a router
- Test connectivity with inter-VLAN routing

Introduction

In this activity, you will configure Router-on-a-Stick inter-VLAN routing. R1 has one connection to S1. S1 and R1 already have basic configurations. The user EXEC password is **cisco,** and the privileged EXEC password is **class**. You will complete the configuration by adding VLANs to S1 and assigning VLANs to the correct ports. Then you will configure R1 with subinterfaces, 802.1Q encapsulation, and IP addressing.

Task 1: Test Connectivity without Inter-VLAN Routing

Step 1. Ping between PC1 and PC3.

Wait for switch convergence. The link lights on the switch connecting to PC1 and PC3 change from amber to green. When the link lights are green, ping between PC1 and PC3. Because the two PCs are on separate networks and inter-VLAN routing is not configured, they cannot communicate with one another, so the ping fails.

Step 2. Switch to simulation mode to monitor pings.

- Switch to simulation mode by selecting the **Simulation** tab or pressing **Shift+S**.
- Click **Capture/Forward** to see the steps the ping takes between PC1 and PC3.
- Notice how the ping cannot even cross the switch.

Your completion percentage should be 0%.

Task 2: Add VLANs

Step 1. Create VLANs on S1.

Create VLAN 10 and VLAN 30 on S1. PC1 belongs to VLAN 10, and PC2 belongs to VLAN 30. To create the VLANs, issue the **vlan 10** and **vlan 30** commands in global configuration mode.

```
S1#configure terminal
S1(config)#vlan 10
S1(config-vlan)#vlan 30
```

To check whether the VLANs were created, issue the **show vlan brief** command from the privileged EXEC prompt.

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10   VLAN0010                          active
30   VLAN0030                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 2. Assign the VLANs to ports.

Each port is assigned to a VLAN to allow for inter-VLAN communication. The Fa0/11 interface belongs to VLAN 10, and the Fa0/6 interface belongs to VLAN 30.

To assign a VLAN to a port, enter interface configuration mode. For Fa0/11, the command is **interface fa0/11**. Issue the **switchport mode access** command to set the port to access mode. The **switchport access vlan 10** command assigns VLAN 10 to that port.

```
S1(config-if)#interface fa0/11
S1(config-if)#switchport mode access
```



```
S1(config-if)#switchport access vlan 10
```

Repeat the steps for the Fa0/6 interface for VLAN 30.

```
S1(config)#interface fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
```

The Fa0/5 port on S1 is set to trunk, which allows it to carry information from both VLAN 10 and VLAN 30. From the Fa0/5 interface, issue the **switchport mode trunk** command to set the port to trunk. Packet Tracer does not grade this command, but it is necessary in configuring inter-VLAN routing.

```
S1(config-if)#interface fa0/5
S1(config-if)#switchport mode trunk
```

Step 3. Test connectivity between PC1 and PC3.

Now issue a ping between PC1 and PC3. The ping should still fail.

Step 4. Check results.

Your completion percentage should be 27%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure IP addressing

Step 1. Configure subinterfaces with 802.1Q encapsulation.

Create two subinterfaces on R1: Fa0/1.10 and Fa0/1.30. These subinterfaces are assigned to VLANs. To create the first subinterface, enter subinterface configuration mode for Fa0/1.10 by issuing the **interface fa0/1.10** command. Notice that the router prompt changes.

While in subinterface configuration mode, issue the **encapsulation dot1Q 10** command to set the encapsulation type to 802.1Q and assign VLAN 10 to the virtual interface.

Assign the correct IP address to the port. For Fa0/1.10, it is 172.17.10.1 with a subnet mask of 255.255.255.0.

Repeat these steps for the Fa0/1.30 interface using the correct IP address and VLAN ID.

```
R1(config)#interface fa0/1.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface fa0/1.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
```

Step 2. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Test Connectivity Again

Step 1. Ping between PC1 and PC3.

Ping from PC1 to PC3. The ping should succeed.

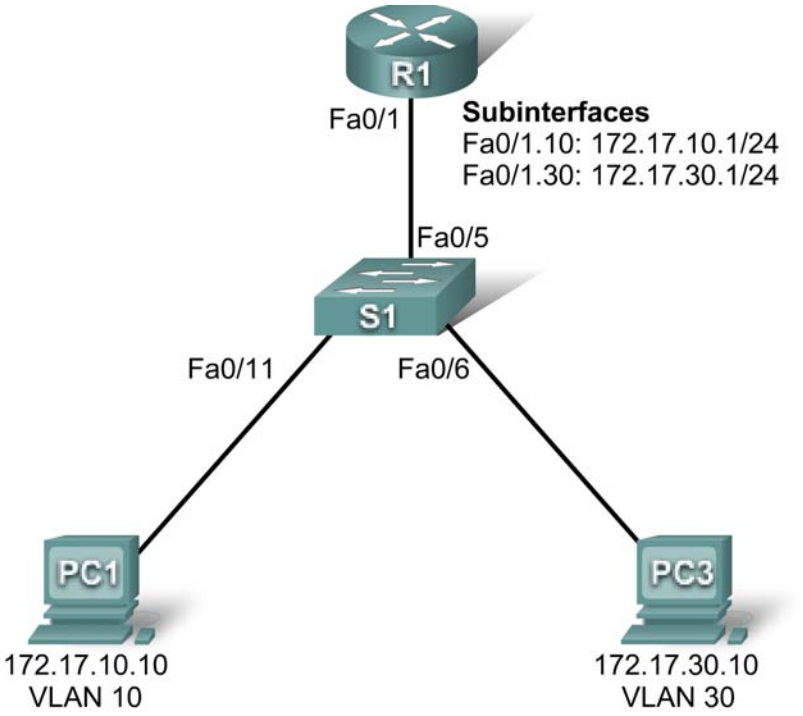
Step 2. Switch to simulation mode to monitor pings.

- Switch to simulation mode by selecting the **Simulation** tab or pressing **Shift+S**.

- Click **Capture/Forward** to see the steps the ping takes between PC1 and PC3.
- Watch how the ping goes from PC1 through S1 first, then to R1, then back to S1, and finally to the PC3.

PT Activity 6.3.3: Troubleshooting Inter-VLAN Routing

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/1.10**	172.17.10.1	255.255.255.0	N/A
	Fa0/1.30	172.17.30.1	255.255.255.0	N/A
PC1	**NIC**	172.17.10.10	255.255.255.0	172.17.10.1
PC3	**NIC**	172.17.30.10	255.255.255.0	172.17.30.1

Learning Objectives

- Test connectivity between PCs and a router
- Gather data on the problem
- Implement the solution and test connectivity

Introduction

In this activity, you will troubleshoot connectivity problems between PC1 and PC3. The activity is complete when you achieve 100% and the two PCs can ping each other. Any solution you implement must conform to the topology diagram.

Task 1: Test Connectivity between PCs and a Router

Use the **Add Simple PDU** tool to ping between two PCs on the same VLAN. The following tests should be successful at the conclusion of this activity:

- PC1 can ping R1
- PC3 can ping R1
- PC1 can ping PC3

Can PC1 ping R1? _____

Can PC3 ping R1? _____

Can PC1 ping PC3? _____

Task 2: Gather Data on the Problem

Step 1. Verify the configuration on the PCs.

Are the following configurations for each PC correct?

- IP address
- Subnet mask
- Default gateway

Step 2. Verify the configuration on S1.

Are the configurations on the switch correct? Be sure to verify the following:

- Ports assigned to the correct VLANs
- Ports configured for the correct mode
- Ports connected to the correct device

Step 3. Verify the configuration on R1.

Are the configurations on the router correct? Be sure to verify the following:

- IP addresses
- Interface status
- Encapsulation and VLAN assignment

Step 4. Document the problem and suggest solutions.

What are the reasons why connectivity failed between the PCs? What are the solutions? There could be more than one problem and more than one solution. All solutions must conform to the topology diagram.

PC1 and/or PC3

Problem: _____

Solution: _____

S1

Problem: _____

Solution: _____

R1

Problem: _____

Solution: _____

Task 3: Implement the Solution and Test Connectivity

Step 1. Make changes according to the suggested solutions in Task 2.

Note: If you make changes to the switch configuration, you should make the changes in Realtime mode rather than Simulation mode. This is necessary so that the switch port will proceed to the forwarding state.

Step 2. Test connectivity between PCs and R1.

If you change any IP configurations, you should create new pings because the prior pings use the old IP address.

- PC1 should be able to ping R1
- PC3 should be able to ping R1
- PC1 should be able to ping PC3

Can PC1 ping R1? _____

Can PC3 ping R1? _____

Can PC1 ping PC3? _____

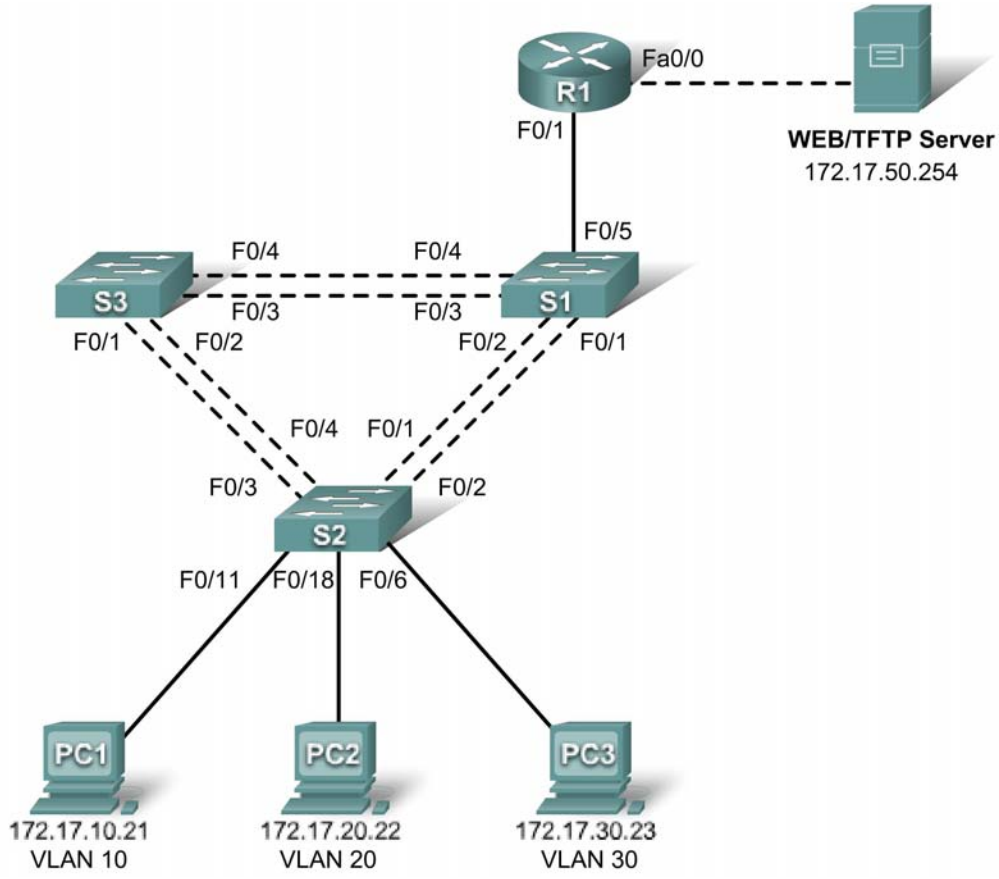
If any pings fail, return to Task 2 to continue troubleshooting.

Step 3. Check completion percentage.

Your completion percentage should be 100%. If not, return to Step 1 and continue to implement your suggested solutions. You will not be able to click **Check Results** and see which required components are not yet completed.

PT Activity 6.4.1: Basic Inter-VLAN Routing

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	172.17.99.11	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.12	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.13	255.255.255.0	172.17.99.1
R1	**Fa0/0**	See Interface Configuration Table		N/A
	Fa0/1	172.17.50.1	255.255.255.0	N/A
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
Server	**NIC**	172.17.50.254	255.255.255.0	172.17.50.1

Port Assignments – S2

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 - 0/10	VLAN 30 – Guests(Default)	172.17.30.0 /24
Fa0/11 - 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Students	172.17.20.0 /24

Subinterface Configuration Table – R1

Interface	Assignment	IP Address
Fa0/0.1	VLAN 1	172.17.1.1 /24
Fa0/0.10	VLAN 10	172.17.10.1 /24
Fa0/0.20	VLAN 20	172.17.20.1 /24
Fa0/0.30	VLAN 30	172.17.30.1 /24
Fa0/0.99	VLAN 99	172.17.99.1 /24

Learning Objectives

- Perform basic switch configurations
- Configure the Ethernet interfaces on the host PCs
- Configure VTP on the switches
- Configure the router and the remote server LAN

Introduction

In this activity, you will perform basic switch configurations, configure addressing on PCs, configure VTP and inter-VLAN routing.

Task 1: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the addressing table and the following guidelines:

- Configure the switch hostname.
- Disable DNS lookup.
- Configure the default gateway.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
- Configure the default gateway on each switch.

```
Switch>enable
Switch#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
```



```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
```

Task 2: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2 and PC3 with the IP addresses from the addressing table.

Task 3: Configure VTP on the Switches

Step 1. Enable the user ports on S2 in access mode.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

Step 2. Configure VTP.

Configure VTP on the three switches using the following table. Remember that VTP domain names and passwords are case-sensitive.

Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Server	Lab5	cisco
S2	Client	Lab5	cisco
S3	Client	Lab5	cisco

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end

S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
```



```
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end

S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Step 3. Configure trunking ports and designate the native VLAN for the trunks.

Configure Fa0/1 through Fa0/5 as trunking ports, and designate VLAN 99 as the native VLAN for these trunks. When this activity was started, these ports were disabled and must be re-enabled now using the **no shutdown** command.

Only the commands for the FastEthernet0/1 interface on each switch are shown, but the commands should be applied up to the FastEthernet0/5 interface.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config)#end

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#no shutdown
S2(config-if)#end

S3(config)#interface fa0/1
S3(config-if#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#no shutdown
S3(config-if-#end
```

Step 4. Configure the VTP server with VLANs.

Configure the following VLANS on the VTP server:

VLAN	VLAN Name
VLAN 99	management
VLAN 10	faculty-staff
VLAN 20	students
VLAN 30	guest

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config)#vlan 10
S1(config-vlan)#name faculty-staff
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config)#vlan 30
```



```
S1(config-vlan)#name guest
S1(config-vlan)#end
```

Verify that the VLANs have been created on S1 with the show vlan brief command.

Step 5. Verify that the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to verify that all four VLANs have been distributed to the client switches.

```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
10   faculty/staff                     active
20   students                          active
30   guest                             active
99   management                        active

S3#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10   faculty-staff                     active
20   students                          active
30   guest                             active
99   management                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 6. Configure the management interface address on all three switches.

```
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0

S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0

S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? _____

If not, troubleshoot the switch configurations and try again.

Step 7. Assign switch ports to VLANs on S2.

Port assignments are listed in the table at the beginning of the activity. However, since Packet Tracer 4.11 does not support the **interface range** command, only assign the first port from each range.

```
S2(config)#interface fa0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fa0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fa0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S2#
```

Step 8. Check connectivity between VLANs.

Open the Command Prompt on the three PCs.

- Ping from PC1 to PC2 (172.17.20.22)
- Ping from PC2 to PC3 (172.17.30.23)
- Ping from PC3 to PC1 (172.17.30.21)

Are the pings successful? _____

If not, why do these pings fail?

Task 4: Configure the Router and the Remote Server LAN

Step 1. Create a basic configuration on the router.

- Configure the router with hostname R1.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2. Configure the trunking interface on R1.

You have demonstrated that connectivity between VLANs requires routing at the network layer, exactly like connectivity between any two remote networks. There are a couple of options for configuring routing between VLANs.

The first is something of a brute force approach. An L3 device, either a router or a Layer 3 capable switch, is connected to a LAN switch with multiple connections--a separate connection for each VLAN that requires inter-VLAN connectivity. Each of the switch ports used by the L3 device are configured in a different VLAN on the switch. After IP addresses are assigned to the interfaces on the L3 device, the routing table has directly connected routes for all VLANs, and inter-VLAN routing is enabled. The limitations to this approach are the lack of sufficient Fast Ethernet ports on routers, under-utilization of ports on L3 switches and routers, and excessive wiring and manual configuration. The topology used in this lab does not use this approach.

An alternative approach is to create one or more Fast Ethernet connections between the L3 device (the router) and the distribution layer switch, and to configure these connections as **dot1q** trunks. This allows all inter-VLAN traffic to be carried to and from the routing device on a single trunk. However, it requires that the L3 interface be configured with multiple IP addresses. This can be done by creating virtual interfaces, called subinterfaces, on one of the router Fast Ethernet ports and configuring them to be **dot1q** aware.

Using the subinterface configuration approach requires these steps:

- Enter subinterface configuration mode
- Establish trunking encapsulation
- Associate a VLAN with the subinterface
- Assign an IP address from the VLAN to the subinterface

The commands are as follows:

```
R1(config)#interface fastethernet 0/0
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/0.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Note the following points in this configuration:

- The physical interface is enabled using the **no shutdown** command, because router interfaces are down by default. The subinterface will then be up by default.
- The subinterface can use any number that can be described with 32 bits, but it is good practice to assign the number of the VLAN as the interface number, as has been done here.
- The native VLAN is specified on the L3 device so that it is consistent with the switches. Otherwise, VLAN 1 is native by default, and there is no communication between the router and the management VLAN on the switches.

Step 3. Configure the server LAN interface on R1.

```
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 172.17.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

There are now six networks configured. Verify that you can route packets to all six by checking the routing table on R1.

```
R1#show ip route
<output omitted>
```



```
Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 6 subnets
C       172.17.1.0 is directly connected, FastEthernet0/0.1
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.20.0 is directly connected, FastEthernet0/0.20
C       172.17.30.0 is directly connected, FastEthernet0/0.30
C       172.17.50.0 is directly connected, FastEthernet0/1
C       172.17.99.0 is directly connected, FastEthernet0/0.99
```

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

Step 4. Verify Inter-VLAN routing.

From PC1, verify that you can ping the remote server (172.17.50.254) and the other two hosts (172.17.20.22 and 172.17.30.23). It may take a couple of pings before the end-to-end path is established.

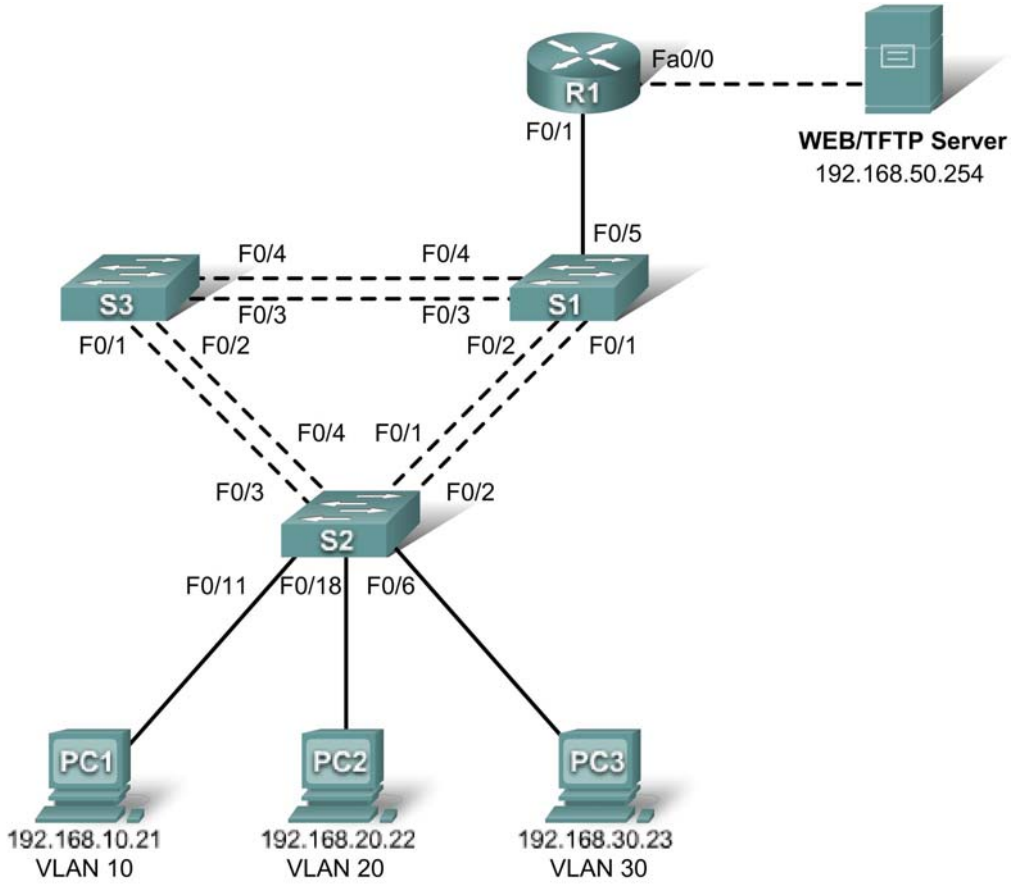
These pings should be successful. If not, troubleshoot your configuration. Check to make sure that the default gateways have been set on all PCs and all switches.

Task 5: Reflection

In Task 4, you configured VLAN 99 as the native VLAN in the router Fa0/0.99 interface configuration. Why would packets from the router or hosts fail when trying to reach the switch management interfaces if the native VLAN were left in default?

PT Activity 6.4.2: Challenge Inter-VLAN Routing

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	192.168.99.11	255.255.255.0	192.168.99.1
S2	**VLAN 99**	192.168.99.12	255.255.255.0	192.168.99.1
S3	**VLAN 99**	192.168.99.13	255.255.255.0	192.168.99.1
R1	**Fa0/0**	192.168.50.1	255.255.255.0	N/A
	Fa0/1	See Interface Configuration Table		N/A
PC1	**NIC**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**NIC**	192.168.30.23	255.255.255.0	192.168.30.1
Server	**NIC**	192.168.50.254	255.255.255.0	192.168.50.1

Port Assignments – S2

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks (Native VLAN 99)	192.168.99.0 /24
Fa0/6 - 0/10	VLAN 30 – Sales	192.168.30.0 /24
Fa0/11 - 0/17	VLAN 10 – R&D	192.168.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Engineering	192.168.20.0 /24

Interface Configuration Table – R1

Interface	Assignment	IP Address
Fa0/0.1	VLAN 1	192.168.1.1 /24
Fa0/0.10	VLAN 10	192.168.10.1 /24
Fa0/0.20	VLAN 20	192.168.20.1 /24
Fa0/0.30	VLAN 30	192.168.30.1 /24
Fa0/0.99	VLAN 99	192.168.99.1 /24

Learning Objectives

- Perform basic switch configurations
- Configure the Ethernet interfaces on the server and host PCs
- Configure VTP on the switches
- Configure the router

Introduction

In this activity, you will perform basic switch configurations, configure VTP, trunking, configure subinterfaces, and demonstrate inter-VLAN routing.

Task 1: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console and vty connections.
- Configure the default gateway on each switch.

Task 2: Configure the Ethernet Interfaces on the Server and Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3 and the remote TFTP/Web Server with the IP addresses from the addressing table. Connect these devices using the correct cables and interfaces.

Task 3: Configure VTP on the Switches

Step 1. Configure VTP on the three switches.

Use the following table to configure the switches. Remember that VTP domain names and passwords are case-sensitive.

Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Server	Lab5	cisco
S2	Client	Lab5	cisco
S3	Client	Lab5	cisco

Step 2. Configure trunking ports and designate the native VLAN for the trunks.

Configure Fa0/1 through Fa0/5 as trunking ports, and designate VLAN 99 as the native VLAN for these trunks.

Step 3. Configure VLANs on the VTP server.

Configure the following VLANs on the VTP server.

VLAN	VLAN Name
VLAN 99	Management
VLAN 10	R&D
VLAN 20	Engineering
VLAN 30	Sales

Verify that the VLANs have been created on S1 with the **show vlan brief** command.

Step 4. Verify that the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to verify that the four VLANs have been distributed to the client switches.

Step 5. Configure the Management interface address on all three switches.

Refer to the addressing table and assign IP addressing to the three switches.

Verify that the switches are correctly configured by pinging between them. From S1, ping the Management interface on S2 and S3. From S2, ping the Management interface on S3.

Were the pings successful? _____

If not, troubleshoot the switch configurations and resolve.

Step 6. Assign switch ports to VLANs on S2.

Refer to the port assignment table to assign ports to VLANs on S2.

Step 7. Check connectivity between VLANs.

Open command windows on the three hosts connected to S2. Ping from PC1 (192.168.10.21) to PC2 (192.168.20.22). Ping from PC2 to PC3 (192.168.30.23).

Are the pings successful? _____

If not, why do these pings fail?

_____

Task 4: Configure the Router

Step 1. Create a basic configuration on the router.

- Configure the router with hostname R1.
- Disable DNS lookup.
- Configure an EXEC mode secret of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2. Configure the trunking interface on R1.

Configure the Fa0/1 interface on R1 with five subinterfaces, one for each VLAN identified in the Subinterface Configuration Table at the beginning of the activity. Configure these subinterfaces with dot1q encapsulation, and use the first address in each VLAN subnet on the router subinterface. Specify VLAN 99 as the native VLAN on its subinterface. Do not assign an IP address to the physical interface, but be sure to enable it. Document your subinterfaces and their respective IP addresses in the subinterface table.

Step 3. Configure the server LAN interface on R1.

Refer to the addressing table and configure Fa0/0 with the correct IP address and mask. Describe the interface as **server interface**.

Step 4. Verify the routing configuration.

At this point, there should be six networks configured on R1. Verify that you can route packets to all six by checking the routing table on R1.

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

Step 5. Verify inter-VLAN routing

From PC1, verify that you can ping the remote server (192.168.50.254) and the other two hosts (192.168.20.22 and 192.168.30.23). It may take a couple of pings before the end-to-end path is established.

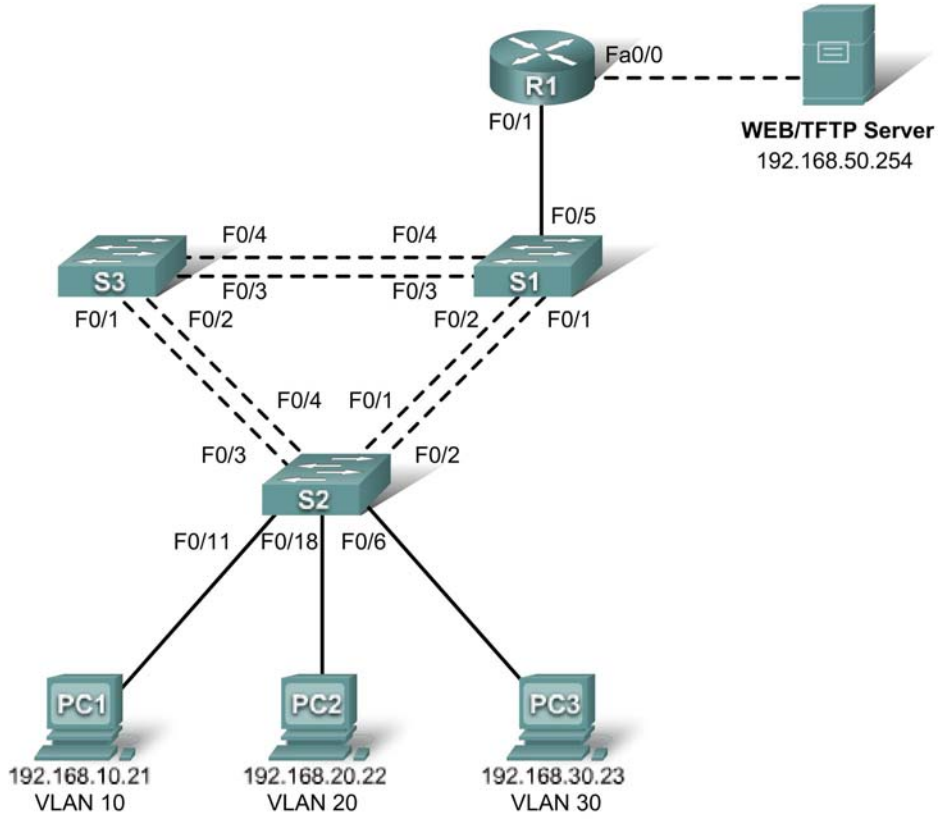
Are the pings successful? _____

If not, troubleshoot your configuration. Check to make sure the default gateways have been set on all PCs and all switches. If any of the hosts have gone into hibernation, the connected interface may go down.

At this point, you should be able to ping any node on any of the six networks configured on your LAN, including the switch management interfaces.

PT Activity 6.4.3: Troubleshooting Inter-VLAN Routing

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	**VLAN 99**	192.168.99.11	255.255.255.0	192.168.99.1
S2	**VLAN 99**	192.168.99.12	255.255.255.0	192.168.99.1
S3	**VLAN 99**	192.168.99.13	255.255.255.0	192.168.99.1
R1	**Fa0/0**	192.168.50.1	255.255.255.0	N/A
	Fa0/1	See Interface Configuration Table		N/A
PC1	**NIC**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**NIC**	192.168.30.23	255.255.255.0	192.168.30.1
Server	**NIC**	192.168.50.254	255.255.255.0	192.168.50.1

Port Assignments – S2

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks (Native VLAN 99)	192.168.99.0 /24
Fa0/6 - 0/10	VLAN 30 – Sales	192.168.30.0 /24
Fa0/11 - 0/17	VLAN 10 – R&D	192.168.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Engineering	192.168.20.0 /24

Interface Configuration Table – R1

Interface	Assignment	IP Address
Fa0/0.1	VLAN 1	192.168.1.1 /24
Fa0/0.10	VLAN 10	192.168.10.1 /24
Fa0/0.20	VLAN 20	192.168.20.1 /24
Fa0/0.30	VLAN 30	192.168.30.1 /24
Fa0/0.99	VLAN 99	192.168.99.1 /24

Learning Objectives

- Troubleshoot and correct the Inter-VLAN issues and configuration errors
- Document the network configuration

Introduction

In this activity, you will troubleshoot the network, find and correct all configuration errors, and document the corrected network.

Task 1: Troubleshoot and Correct the Inter-VLAN Issues and Configuration Errors

Begin by identifying what is working and what is not:

What is the state of the interfaces?

_____

What hosts can ping other hosts?

_____

Which hosts can ping the server?

_____

What routes should be in the R1 routing table?

_____

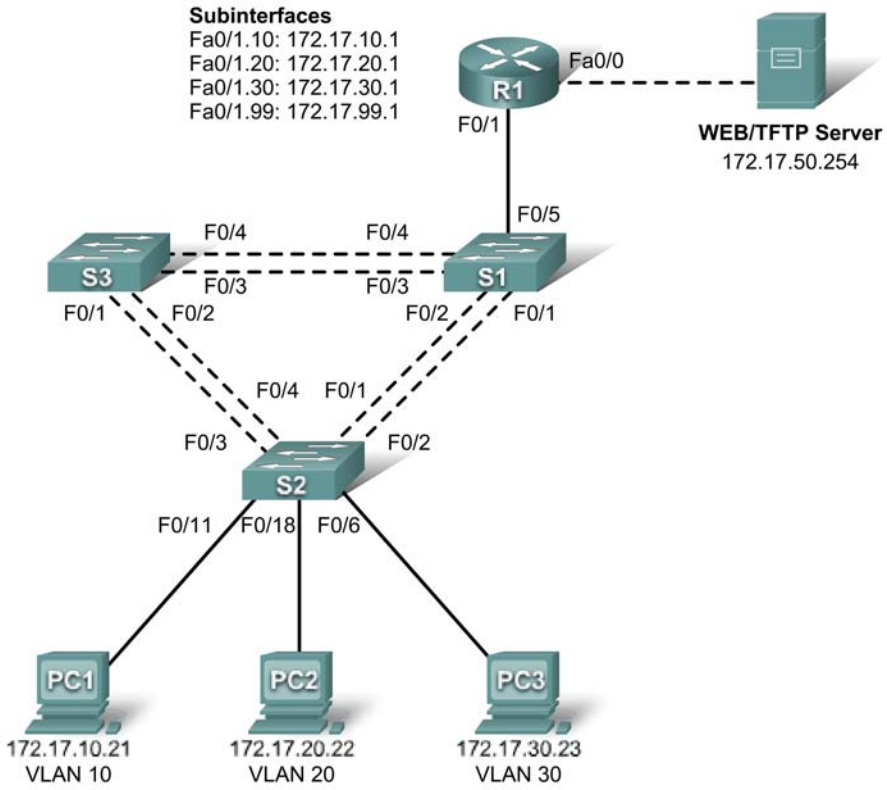
When all errors are corrected, you should be able to ping the remote server from any PC or any switch. In addition, you should be able to ping between the three PCs and ping the management interfaces on switches from any PC.

Task 2: Document the Network Configuration

When you have successfully completed your troubleshooting, capture the output of the router and all three switches with the **show run** command and save it to a text file.

PT Activity 6.5.1: Packet Tracer Skills Integration Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	172.17.50.1	255.255.255.0	N/A
	Fa0/1.10	172.17.10.1	255.255.255.0	N/A
	Fa0/1.20	172.17.20.1	255.255.255.0	N/A
	Fa0/1.30	172.17.30.1	255.255.255.0	N/A
	Fa0/1.99	172.17.99.1	255.255.255.0	N/A
S1	**VLAN 99**	172.17.99.31	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.32	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.33	255.255.255.0	172.17.99.1
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1

Learning Objectives

- Configure and verify basic device configurations
- Configure VTP
- Configure trunking
- Configure VLANs
- Assign VLANs to ports
- Configure STP
- Configure router-on-a-stick Inter-VLAN routing
- Verify end-to-end connectivity

Introduction

In this activity, you will demonstrate and reinforce your ability to configure switches and routers for inter-VLAN communication. Among the skills you will demonstrate are configuring VLANs, VTP, and trunking on switches. You will also administer STP on switches and configure a router-on-a-stick using subinterfaces.

Task 1: Configure and Verify Basic Device Configurations

Step 1: Configure basic commands.

Configure the router and each switch with the following basic commands. Packet Tracer grades only the hostnames and default gateways.

- Hostnames
- Banner
- Enable secret password
- Line configurations
- Service encryption
- Switch default gateways

Step 2: Configure the management VLAN interface on S1, S2, and S3.

Create and enable interface VLAN 99 on each switch. Use the addressing table for address configuration.

Step 3: Check results.

Your completion percentage should be 17%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure VTP

Step 1: Configure the VTP mode on all three switches.

Configure S1 as the server. Configure S2 and S3 as clients.

Step 2: Configure the VTP domain name on all three switches.

Use **CCNA** as the VTP domain name.

Step 3: Configure the VTP domain password on all three switches.

Use **cisco** as the VTP domain password.

Step 4: Check results.

Your completion percentage should be 28%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Trunking

Step 1: Configure trunking on S1, S2, and S3.

Configure the appropriate interfaces in trunking mode and assign VLAN 99 as the native VLAN.

Step 2: Check results.

Your completion percentage should be 62%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure VLANs

Step 1: Create the VLANs on S1.

Create and name the following VLANs on S1 only. VTP advertises the new VLANs to S1 and S2.

- VLAN 10 **Faculty/Staff**
- VLAN 20 **Students**
- VLAN 30 **Guest(Default)**
- VLAN 99 **Management&Native**

Step 2: Verify that VLANs have been sent to S2 and S3.

Use the appropriate commands to verify that S2 and S3 now have the VLANs you created on S1. It may take a few minutes for Packet Tracer to simulate the VTP advertisements.

Step 3: Check results.

Your completion percentage should be 67%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Assign VLANs to Ports

Step 1: Assign VLANs to access ports on S2.

Assign the PC access ports to VLANs:

- VLAN 10: PC1 connected to Fa0/11
- VLAN 20: PC2 connected to Fa0/18
- VLAN 30: PC3 connected to Fa0/6

Step 2: Verify the VLAN implementation.

Use the appropriate commands to verify your VLAN implementation.

Step 3: Check results.

Your completion percentage should be 75%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure STP

Step 1: Ensure S1 is the root bridge.

Set priorities to 4096.

Step 2: Verify that S1 is the root bridge.

Step 3: Check results.

Your completion percentage should be 82%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure Router-on-a-Stick Inter-VLAN Routing

Step 1: Configure the subinterfaces.

Configure the Fa0/1 subinterfaces on R1 using the information from the addressing table.

Step 2: Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Verify End-to-End Connectivity

Step 1: Verify that PC1 and Web/TFTP Server can ping each other.

Step 2: Verify that PC1 and PC2 can ping each other.

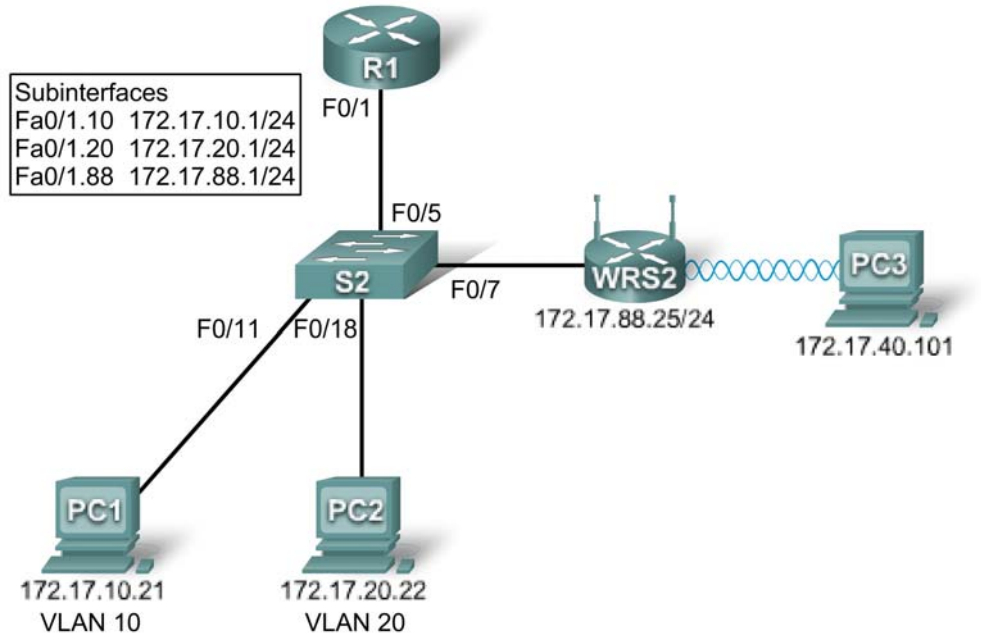
Step 3: Verify that PC3 and PC1 can ping each other.

Step 4: Verify that PC2 and PC3 can ping each other.

Step 5: Verify that the switches can ping R1.

PT Activity 7.3.2: Configuring Wireless LAN Access

Topology Diagram



Learning Objectives

- Add a wireless router to the network
- Configure options in the Linksys Setup tab
- Configure options in the Linksys Wireless tab
- Configure options in the Linksys Administration tab
- Add wireless connectivity to a PC
- Test connectivity

Introduction

In this activity, you will configure a Linksys wireless router, allowing for remote access from PCs as well as wireless connectivity with WEP security.

Task 1: Add a Wireless Router to the Network

Step 1. Add a Linksys WRT300N to the network.

Click **Wireless Devices** in the Device Manager and select Linksys-WRT300N. Add the device between the switch and PC3, as shown in the topology diagram.

Step 2. Configure the display name.

Click the Linksys router to open the configuration GUI. Select the Config tab and set the display name to WRS2.

Step 3. Connect the Internet interface to S1.

Using a straight-through cable, connect the Internet interface of the Linksys router to the Fa0/7 interface of the switch.

Step 4. Check results.

Your completion percentage should be 19%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Options in the Linksys Setup Tab

Step 1. Set the Internet connection type to static IP.

- Click on the Linksys router, and then select the GUI tab.
- In the Setup screen for the Linksys router, locate the Internet Connection Type option under Internet Setup. Click the drop-down menu and select Static IP from the list.

Step 2. Configure the VLAN 88 IP address, subnet mask, and default gateway for WRS2.

- Set the Internet IP address to 172.17.88.25.
- Set the subnet mask to 255.255.255.0.
- Set the default gateway to 172.17.88.1.

Note: Typically in a home or small business network, this Internet IP address is assigned by the ISP through DHCP.

Step 3. Configure the router IP parameters.

- In the **Setup** screen, scroll down to **Network Setup**. For the **Router IP** option, set the IP address to 172.17.40.1 and the subnet mask to 255.255.255.0.
- Under the **DHCP Server Setting**, make sure that the DHCP server is enabled.

Step 4. Save settings.

Click the **Save Settings** button at the bottom of the **Setup** screen.

Note that the IP address range for the DHCP pool adjusts to a range of addresses to match the router IP parameters. These addresses are used for wireless clients. Clients receive an IP address and mask and are given the router IP to use as a gateway.

Step 5. Check results.

Your completion percentage should be 50%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Options in the Linksys Wireless Tab

Step 1. Set the network name (SSID).

- Click the **Wireless** tab.
- Under **Network Name (SSID)**, rename the network from Default to WRS_LAN.
- Click **Save Setting**s.

Step 2. Set the security mode.

- Click **Wireless Security**. It is located next to Basic Wireless Settings in the main Wireless tab.
- Change **Security Mode** from Disabled to WEP.

- Using the default Encryption of 40/64-Bit, set **Key1** to 0123456789
- Click **Save Settings**.

Step 3. Check results.

Your completion percentage should be 69%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure Options in the Linksys Administration Tab

Step 1. Set the router password.

- Click the **Administration** tab.
- Under **Router Access**, change the router password to cisco123. Re-enter the same password to confirm.

Step 2. Enable remote management.

- Under **Remote Access**, enable remote management.
- Click **Save Settings**.

Note: PC1 and PC2 can ping WRS2, but will not be able to remotely manage it through the Internet interface. By default, the WRT300N blocks all attempts to access the web interface from the outside world. Currently, Packet Tracer does not support disabling this security feature. You will test remote management once PC3 wireless connectivity is established.

Step 3. Check results.

Your completion percentage should be 75%. If not, click **Check Results** to see which required components are not yet completed.

Close the web browser on the PC.

Task 5: Add Wireless Connectivity to a PC

Step 1. Remove the Fast Ethernet NIC on PC3.

- Click **PC3** and then click the **Physical** tab.
- In the Physical Device View is an image of the PC. Click the power button on the PC to turn it off.
- Remove the Fast Ethernet NIC by dragging it to the bottom right corner of the window. The NIC is located at the bottom of the machine.

Step 2. Install the wireless NIC on PC3.

- Under **Modules**, find Linksys-WMP300N and drag and drop it where the Fast Ethernet NIC was located.
- Turn the power back on.

Step 3. Configure PC3 with a WEP key.

- In the configuration GUI for PC3, click the **Desktop** tab.
- Click PC Wireless to begin setting up the WEP key for PC3. A Linksys screen is displayed. You should see that the PC has not associated with an access point.
- Click the **Connect** tab.

- The WRS_LAN should appear in the list of available wireless networks. Make sure it is selected and click **Connect**.
- Under **WEP Key 1**, type the WEP, ciscoccna1**,** and click **Connect**.
- Go to the **Link Information** tab. The Signal Strength and Link Quality indicators should show that you have a strong signal.
- Click the **More Information** button to see details of the connection. You see the IP address the PC received from the DHCP pool.
- Close the PC Wireless configuration window.

Step 4. Check results.

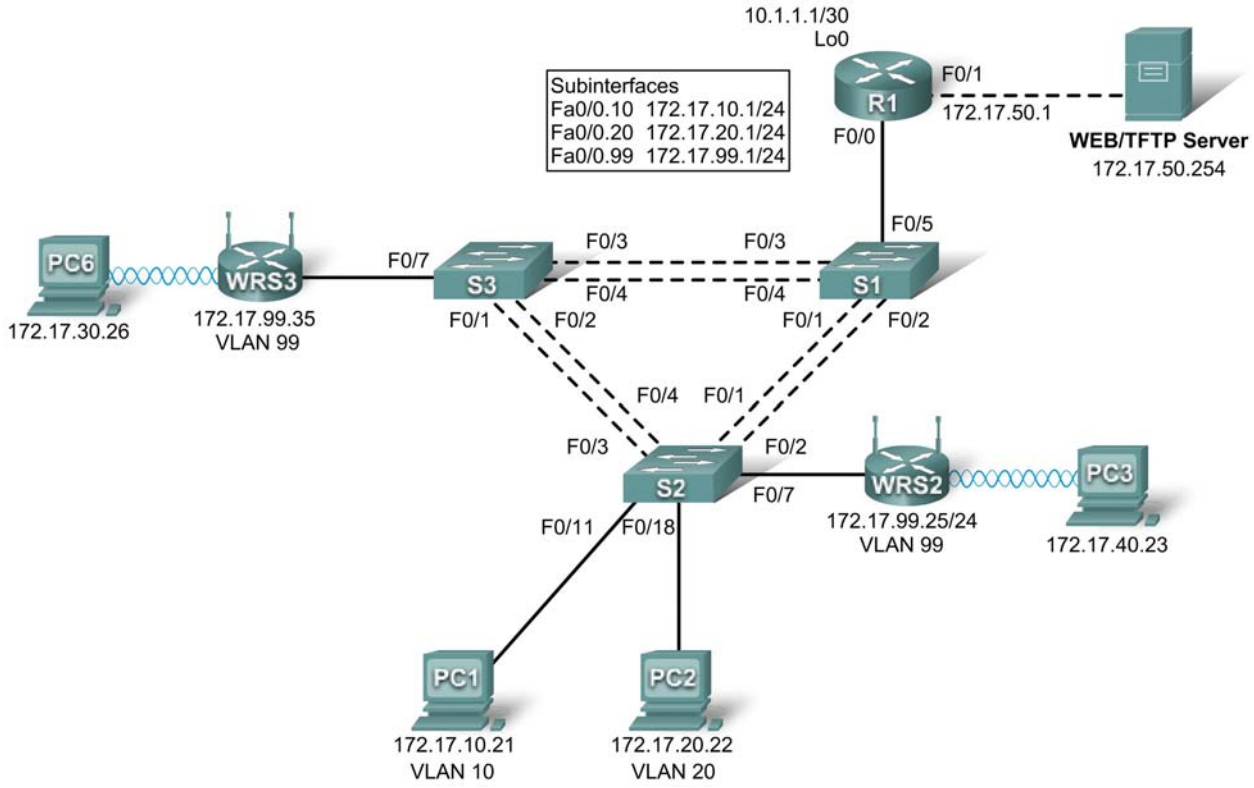
Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Test Connectivity

All the PCs should have connectivity with one another. Click **Check Results,** and then click the **Connectivity Tests** tab to check. If the completion percentage is at 100% but the connectivity tests are unsuccessful, try turning PC3 off and then on again.

PT Activity 7.5.2: Challenge Wireless WRT300N

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/1**	172.17.50.1	255.255.255.0	N/A
	Fa0/0.10	172.17.10.1	255.255.255.0	N/A
	Fa0/0.20	172.17.20.1	255.255.255.0	N/A
	Fa0/0.99	172.17.99.1	255.255.255.0	N/A
	Lo0	10.1.1.1	255.255.255.252	N/A
WRS2	**WAN**	172.17.99.25	255.255.255.0	172.17.99.1
	LAN/Wireless	172.17.40.1	255.255.255.0	N/A
WRS3	**WAN**	172.17.99.35	255.255.255.0	172.17.99.1
	LAN/Wireless	172.17.30.1	255.255.255.0	N/A
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1

VLAN Table

VLAN ID	VLAN Name	Network
VLAN 10	Faculty/Staff	172.17.10.0 /24
VLAN 20	Students	172.17.20.0 /24
VLAN 99	Wireless(Guest)	172.17.99.0 /24

Learning Objectives

- Perform basic router configurations
- Perform switch configurations
- Connect to the Linksys WRT300N router
- Access the WRT300N
- Configure IP settings for the Linksys WRT300N
- Configure DHCP settings
- Basic wireless settings
- Enable wireless security
- Managing and securing the web utility of the router
- Configure WRS2
- Creating and verifying full connectivity
- Configuring port security

Introduction

In this activity, you will configure a Linksys WRT300N, port security on a Cisco switch, and static routes on multiple devices. Make note of the procedures involved in connecting to a wireless network because some changes involve disconnecting clients, which may then have to reconnect after making changes to the configuration.

Task 1: Perform Basic Router Configurations

Step 1. Perform basic router configurations.

Configure R1 according to the following guidelines:

- Router hostname
- Disable DNS lookup
- Configure EXEC mode password of **class**
- Configure a password of **cisco** for console connections
- Configure a password of **cisco** for vty connections

Step 2. Configure router interfaces.

Configure Loopback0, FastEthernet 0/0, 0/1, and any subinterfaces listed in the addressing table. Before configuring the IP addresses on the the subinterfaces, encapsulation must be set to 802.1Q. The VLAN ID is identified by the subinterface number.

Verify the interfaces are up and their IP Addresses are correect with the **show ip interfaces brief** command.

Task 2: Perform Switch Configurations

Step 1. Perform basic switch configurations.

Configure all three switches according to the following:

- Configure hostnames
- Disable DNS lookup
- Configure EXEC mode password of **class**
- Configure a password of **cisco** for console connections
- Configure a password of **cisco** for vty connections

Step 2. Set VTP mode and create VLANs.

For all switches set the VTP mode to **transparent** and create the VLANs according to the table at the beginning of this activity.

Verify the creation of the VLANs with the **show vlan brief** command.

Step 3. Configure switch port interfaces on S1, S2, and S3.

Configure the interfaces on the S1, S2, and S3 switches according to the following:

- Fa0/7 on S2 and S3 are in VLAN 99
- Fa0/5 on S1 is an 802.1Q trunk
- Fa0/11 on S2 is in VLAN 10
- Fa0/18 on S2 is in VLAN 20
- Remaining connected ports are trunk interfaces
- Allow all VLANS across trunking interfaces

Step 4. Verify VLANs and trunking.

Use the **show interfaces trunk** command on S1 and the **show vlan brief** command on S2 to verify that the switches are trunking correctly and the proper VLANs exist.

Step 5. Configure the Ethernet interfaces of PC1 and PC2.

Configure the Ethernet interfaces of PC1 and PC2 with the IP addresses and default gateways according to the addressing table at the beginning of the activity.

Step 6. Test the PC configuration.

Access the Command Prompt on each PC and ping its default gateway. The pings should be successful, if not, troubleshoot.

Task 3: Connect to the Linksys WRT300N Router

Step 1. Connect to a wireless router.

From PC6 access the Desktop then PC Wireless. From here select the Connect tab and connect to the Default network.

Step 2. Verify connectivity settings.

While still at the desktop of the PC, close the Linksys GUI window and then verify the connectivity settings by accessing the Command Prompt and typing the **ipconfig** command.

```
PC>ipconfig
```



```
IP Address.....................: 192.168.1.101
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.1.1

PC>
```

Task 4: Access the WRT300N

Step 1. Access WRS3 through the web browser.

On PC6, close the command prompt and then click the Web Browser. Enter the URL 192.168.1.1, the default gateway of the PC.

Step 2. Enter authentication information.

You will be prompted for a username and password. The default username and password are both **admin**. Once you have entered the login information, you should be viewing the default page of the Linksys WRT300N web utility.

Task 5: Configure IP Settings for the Linksys WRT300N

The best way to understand the following settings is to think of the WRT300N as being similar to a Cisco IOS-based router with two separate interfaces. One of the interfaces, the one configured under Internet Setup, acts as the connection to the switches and the interior of the network. The other interface, configured under Network Setup, acts as the interface connecting to the wireless clients, PC6 and PC3.

Step 1. Set the Internet connection type to static IP.

You should be at the Setup page of the Linksys router. Under Internet Setup is the Internet Connection Type option. Select Static IP.

Step 2. Set the IP address settings for Internet Setup.

- Set the Internet IP address to **172.17.99.35**
- Set the subnet mask to **255.255.255.0**
- Set the default gateway to the Fa0/1 VLAN 99 IP address of R1, **172.17.99.1**

Step 3. Configure the Network Setup IP address to 172.17.30.1 /24

Step 4. Save the settings.

Click **Save Settings**. You are prompted with a "Settings are successful" window. Click Continue. Since the default gateway has changed, PC6 will not be able to access the web utility until its IP address and gateway are updated.

Step 5. Renew IP configuration on PC6.

Close the Web Browser and return to the Desktop of PC6. Again, access the Command Prompt. Type the **ipconfig /renew** command to update PC6's IP address and default gateway.

Note: In Packet Tracer, there must be a space between **ipconfig** and **/renew**.

```
PC>ipconfig /renew

IP Address.....................: 172.17.30.101
Subnet Mask....................: 255.255.255.0
Default Gateway................: 172.17.30.1
```



```
DNS Server.....................: 0.0.0.0

PC>
```

Task 6: Configure DHCP Settings

Now access the wireless router through the web browser again, but this time at the 172.17.30.1 URL.

Under DHCP Server Settings, set the start address to 25 and the maximum number of users to 25.

These settings give any PC that connects to this router wirelessly requesting an IP address through DHCP, an address between 172.17.30.25-49. Only 25 clients at a time are able to get an IP address.

Click **Save Settings** in order for the changes to take place.

Task 7: Basic Wireless Settings

Step 1. Configure the SSID.

Access the Wireless page and change the Network Name SSID from **Default** to **WRS3**.

Step 2. Save settings.

Step 3. Reconnect to the wireless network.

Since the SSID has changed, PC6 is currently unable to access the WRS3 network. On the Desktop return to PC Wireless and select the Connect Tab. Connect to the WRS3 network.

Step 4. Verify the settings.

Now that you have reconnected to the network, you have the new DHCP settings that you configured in Task 6. Verify this at the command prompt with the **ipconfig** command.

```
PC>ipconfig

IP Address.....................: 172.17.30.26
Subnet Mask....................: 255.255.255.0
Default Gateway................: 172.17.30.1
DNS Server.....................: 0.0.0.0

PC>
```

Note: Packet Tracer may need help in updating the IP configuration. If the IP Address is not 172.17.30.26 or the default gateway is wrong, try the **ipconfig /renew** command. If that does not work, return to the Desktop and select IP Configuration. From here switch to Static and back to DHCP. Your settings should match those above.

Task 8: Enable Wireless Security

Step 1. Reconnect to the router setup page (http://172.17.30.1).

Step 2. Navigate to the Wireless page and then select the Wireless Security tab.

Step 3. Under Security Mode, select WEP.

Step 4. Enter a WEP key.

A network is only as secure as its weakest point, and a wireless router is a very convenient place to start

if someone wants to damage your network. By requiring a WEP key to connect to the router, you are adding a level of security.

Unfortunately, there are tools that can crack WEP key encryption. A more robust form of wireless security is WPA and WPA-2, which are currently not supported by Packet Tracer.

Add the WEP key **1234567890**.

Step 5. Save your settings.

You will become disconnected from the network again after saving your settings.

Step 6. Configure PC6 to use WEP authentication.

- Return to the Desktop and click PC Wireless.
- Click on the **Connect** tab.
- From the list of available wireless networks, select **WRS3** and connect.
- A screen will be brought up asking for the WEP. Under WEP Key 1, type the WEP, **1234567890**.
- Click Link Information to verify connectivity to the access point.

Task 9: Managing and Securing the Web Utility of the Router

Step 1. Configure web access password.

Return to the web utility page of the router (http://172.17.30.1) and navigate to the Administration section. Change the router password to **cisco**. Notice how HTTP Web Utility Access is already selected by default. Leave it that way.

Step 2. Save settings.

Task 10: Configure WRS2

Step 1. Connect to WRS2 from PC3.

See Task 3 if you need help.

Step 2. Connect to the Web Utility through the Web Browser.

Access WRS2 through the default gateway, 192.168.2.1.

Step 3. Complete Inernet and Network Setup.

- Assign a Static IP to the Internet interface. Use the addressing from the table at the beginning of the activity.
- Configure the Router IP with the LAN addressing from the table at the beginning of the activity.
- For DHCP Server settings, begin assigning IP Addresses at 172.17.40.22, for up to 25 users.
- Save settings.

Step 4. Renew IP Configuration for PC3.

The **ipconfig /renew** command does not properly renew the IP address from the new DHCP range. Go to IP Configuration on the Desktop and switch to Static then back to DHCP. Verify the new addressing with the **ipconfig** command.

```
PC>ipconfig

IP Address.....................: 172.17.40.23
```



```
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 172.17.40.1

PC>
```

Step 5. Change SSID to WRS2.

Return to the Web Utility and change the SSID to WRS2 under the Wireless page. Be sure to click Save Settings.

Reconnect PC3 to WRS2. See Task 7, Step 3 for help.

Step 6. Configure WEP on WRS2 from Web Utility.

Set the WEP Key to **1234567890** and configure PC3 to use the WEP. See Task 8 for help.

Step 7. Configure web access password to cisco.

See Task 9 for help.

Task 11: Creating and Verifying Full Connectivity

Step 1. Give R1 static routes to the 172.17.30.0 and 172.17.40.0 networks.

These routes will allow R1 to ping the inside Wireless/LAN IP address on the wireless routers.

```
!
ip route 172.17.30.0 255.255.255.0 172.17.99.35
ip route 172.17.40.0 255.255.255.0 172.17.99.25
!
```

Step 2. Verify connectivity.

Verify that R1 has routes to PC3 and PC6 with the **show ip route** command and R1 can ping the inside Wireless/LAN IP address of each wireless router.

Due to a PT bug, PC3 and PC6 will not be able to ping one another.

Task 12: Configuring Port Security

Step 1. Configure PC1 and PC2 port security.

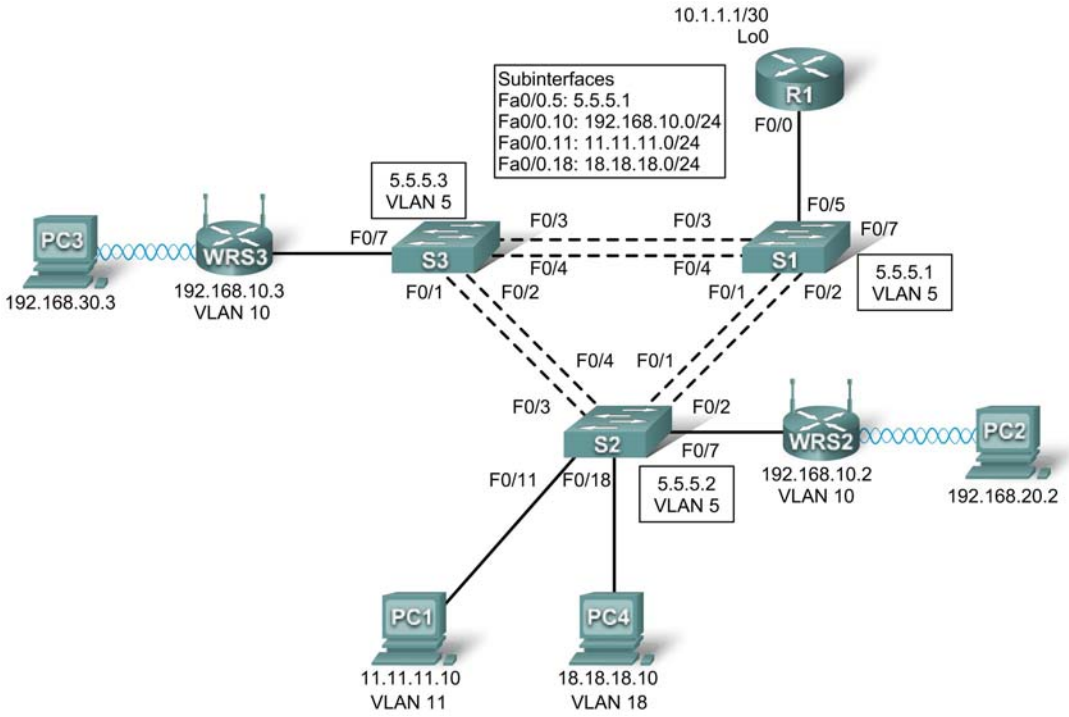
Enable port security and enable dynamic sticky MAC addresses.

Step 2. Generate traffic across the ports by pinging PC2 from PC1.

Step 3. Verify port security.

PT Activity 7.5.3: Troubleshooting Wireless WRT300N

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0.5**	5.5.5.10	255.255.255.0	N/A
	Fa0/0.10	192.168.10.1	255.255.255.0	N/A
	Fa0/0.11	11.11.11.1	255.255.255.0	N/A
	Fa0/0.18	18.18.18.1	255.255.255.0	N/A
	Lo0	10.1.1.1	255.255.255.252	N/A
WRS2	**WAN**	192.168.10.2	255.255.255.0	192.168.10.1
	LAN/Wireless	192.168.20.1	255.255.255.0	N/A
WRS3	**WAN**	192.168.10.3	255.255.255.0	192.168.10.1
	LAN/Wireless	192.168.30.1	255.255.255.0	N/A
PC1	**NIC**	11.11.11.10	255.255.255.0	11.11.11.1
PC4	**NIC**	18.18.18.10	255.255.255.0	18.18.18.1

Addressing Table continued on next page

Addressing Table continued

S1	**VLAN 5**	5.5.5.1	255.255.255.0	N/A
S2	**VLAN 5**	5.5.5.2	255.255.255.0	N/A
S3	**VLAN 5**	5.5.5.3	255.255.255.0	N/A

Learning Objectives

- Troubleshoot the network
- Verify connectivity

Scenario

In this activity, a basic network and wireless network have been configured improperly. You must find and correct the misconfigurations based on the minimum network specifications provided by your company.

Task 1: Troubleshoot the Network

Examine the routers and switches, determine any errors in the network.

Note: Packet Tracer will not grade the allowed VLANs for trunking mode.

The wireless routing requirements are as follows:

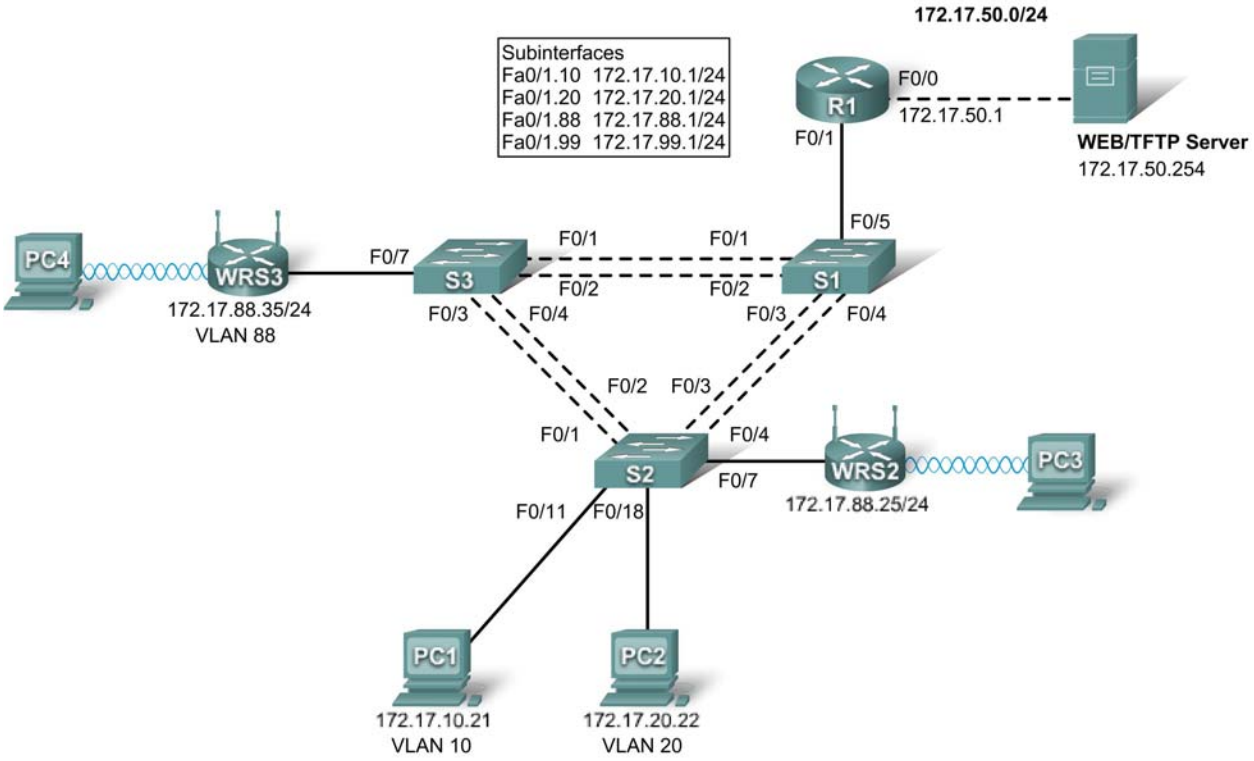
- Connections via the IP addresses shown in the topology diagram.
- 30 clients can get an IP address through DHCP at a single time.
- Wireless clients must be authenticated using WEP with a key of **5655545251**.
- Ping requests coming from outside WAN ports of the Linksys routers to their inside LAN/wireless IP addresses (192.168.30.1) must be successful.
- DHCP must assign PC2 and PC3 their proper IP addresses.

Task 2: Verify Connectivity

Due to a bug, Packet Tracer does not allow for PC2 and PC3 to ping one another, however connectivity should exist in all other circumstances. All the PCs should be able to ping one another and R1. If they do not, continue troubleshooting.

PT Activity 7.6.1: Packet Tracer Skills Integration Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	172.17.50.1	255.255.255.0	N/A
	Fa0/1.10	172.17.10.1	255.255.255.0	N/A
	Fa0/1.20	172.17.20.1	255.255.255.0	N/A
	Fa0/1.88	172.17.88.1	255.255.255.0	N/A
	Fa0/1.99	172.17.99.1	255.255.255.0	N/A
WRS2	**Internet**	172.17.88.25	255.255.255.0	172.17.88.1
	LAN	172.17.40.1	255.255.255.0	N/A
WRS3	**Internet**	172.17.88.35	255.255.255.0	172.17.88.1
	LAN	172.17.30.1	255.255.255.0	N/A

Addressing Table continued on the next page

Addressing Table continued

S1	**VLAN 99**	172.17.99.31	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.32	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.33	255.255.255.0	172.17.99.1
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1

Learning Objectives

- Configure and verify basic device configurations
- Configure VTP
- Configure trunking
- Configure VLANs
- Assign VLAN to ports
- Configure STP
- Configure router-on-a-stick inter-VLAN routing
- Configure wireless connectivity
- Verify end-to-end connectivity

Introduction

In this final Packet Tracer Skills Integration Challenge activity for the Exploration: LAN Switching and Wireless course, you will apply all the skills you have learned including configuring VLANs and VTP, optimizing STP, enabling inter-VLAN routing and integrating wireless connectivity.

Task 1: Configure and Verify Basic Device Configurations

Step 1. Configure basic commands.

Configure each switch with the following basic commands. Packet Tracer only grades the hostnames and default gateways.

- Hostnames
- Banner
- Enable secret password
- Line configurations
- Service encryption
- Switch default gateways

Step 2. Configure the management VLAN interface on S1, S2, and S3.

Create and enable interface VLAN 99 on each switch. Use the addressing table for address configuration.

Step 3. Check results.

Your completion percentage should be 13%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure VTP

Step 1. Configure the VTP mode on all three switches.

Configure S1 as the server. Configure S2 and S3 as clients.

Step 2. Configure the VTP domain name on all three switches.

Use **CCNA** as the VTP domain name.

Step 3. Configure the VTP domain password on all three switches.

Use **cisco** as the VTP domain password.

Step 4. Check results.

Your completion percentage should be 21%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Trunking

Step 1. Configure trunking on S1, S2, and S3.

Configure the appropriate interfaces in trunking mode and assign VLAN 99 as the native VLAN.

Step 2. Check results.

Your completion percentage should be 44%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure VLANs

Step 1. Create the VLANs on S1.

Create and name the following VLANs on S1 only. VTP advertises the new VLANs to S2 and S3.

- VLAN 10 **Faculty/Staff**
- VLAN 20 **Students**
- VLAN 88 **Wireless(Guest)**
- VLAN 99 **Management&Default**

Step 2. Verify that VLANs have been sent to S2 and S3.

Use the appropriate commands to verify that S2 and S3 now have the VLANs you created on S1. It may take a few minutes for Packet Tracer to simulate the VTP advertisements.

Step 3. Check results.

Your completion percentage should be 54%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Assign VLANs to Ports

Step 1. Assign VLANs to access ports on S2 and S3.

Assign the PC access ports to VLANs:

- VLAN 10: PC1
- VLAN 20: PC2

Assign the wireless router access ports to VLAN 88.

Step 2. Verify VLAN implementation.

Use the appropriate commands to verify your VLAN implementation.

Step 3. Check results.

Your completion percentage should be 61%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure STP

Step 1. Ensure that S1 is the root bridge for all spanning tree instances.

Use 4096 priority.

Step 2. Verify that S1 is the root bridge.

Step 3. Check results.

Your completion percentage should be 66%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure Router-on-a-Stick Inter-VLAN Routing

Step 1. Configure subinterfaces.

Configure the Fa0/1 subinterfaces on R1 using the information from the addressing table.

Step 2. Check results.

Your completion percentage should be 79%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Configure Wireless Connectivity

Step 1. Configure IP Addressing for WRS2 and WRS3.

Configure LAN settings and then static addressing on the Internet interfaces for both WRS2 and WRS3 using the addresses from the topology.

Note: A bug in Packet Tracer may prevent you from assigning the static IP address first. A workaround for this issue is to configure the LAN settings first under Network Setup. Save the settings. Then configure the static IP information under Internet Connection Type and save settings again.

Step 2. Configure wireless network settings.

- The SSIDs for the routers are WRS2_LAN and WRS3_LAN, respectively.
- The WEP for both is 12345ABCDE.

Step 3. Configure the wireless routers for remote access.

Configure the administration password as cisco123.

Step 4. Configure PC3 and PC4 to access the network using DHCP.

PC3 connects to the WRS2_LAN, and PC4 connects to the WRS3_LAN.

Step 5. Verify remote access capability.

Step 6. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 9: Verify End-to-End Connectivity

Step 1. Verify that PC1 and Web/TFTP Server can ping each other.

Step 2. Verify that PC1 and PC2 can ping each other.

Step 3. Verify that PC3 and PC1 can ping each other.

Step 4. Verify that PC2 and PC3 can ping each other.

